[H.A.S.C. No. 110–34]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2008

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE HEARING

ON

BUDGET REQUEST ON HARNESSING TECHNOLOGICAL INNOVATION: CHALLENGES AND OPPORTUNITIES

HEARING HELD
MARCH 14, 2007

U.S. GOVERNMENT PRINTING OFFICE
44–898 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

ADAM SMITH, Washington, *Chairman*

MIKE McINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
MARK E. UDALL, Colorado
BRAD ELLSWORTH, Indiana
KIRSTEN E. GILLIBRAND, New York
KATHY CASTOR, Florida

MAC THORNBERRY, Texas
ROBIN HAYES, North Carolina
KEN CALVERT, California
JOHN KLINE, Minnesota
THELMA DRAKE, Virginia
K. MICHAEL CONAWAY, Texas
JIM SAXTON, New Jersey

Kevin Gates, *Professional Staff Member*
Alex Kugajevsky, *Professional Staff Member*
Andrew Tabler, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2007

WEDNESDAY, MARCH 14, 2007

FISCAL YEAR 2008 NATIONAL DEFENSE AUTHORIZATION ACT—BUDGET REQUEST ON HARNESSING TECHNOLOGICAL INNOVATION: CHALLENGES AND OPPORTUNITIES

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

FISCAL YEAR 2008 NATIONAL DEFENSE AUTHORIZATION ACT—BUDGET REQUEST ON HARNESSING TECHNOLOGICAL INNOVATION: CHALLENGES AND OPPORTUNITIES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES SUBCOMMITTEE,
Washington, DC, Wednesday, March 14, 2007.

The subcommittee met, pursuant to call, at 3:00 p.m., in room 2118, Rayburn House Office Building, Hon. Adam Smith (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SMITH. I think we will go ahead and get started and call the meeting formally to order.

I want to thank our witnesses and members.

We have probably an hour-and-a-half, somewhere in that neighborhood, before they are going to call votes over on the floor. It is hard to say precisely. And when they do call votes, it is going to be about an hour's worth, because there is a motion to recommit in there.

The importance of all of that is, we are going to try to get done—when the bells go off, hopefully we will be done with our witnesses and questions, and try to work on that timeframe.

With that, I want to welcome everybody to the Subcommittee on Terrorism, Unconventional Threats and Capabilities. We are hearing today about technological innovations, specifically focusing on the Science and Technology (S&T) programs within the military, and how we can do a better job of making sure we get the absolute best technology to our military and to the warfighter as quickly and efficiently as possible.

I think there is a lot of potential here. Certainly, the military is doing a lot of things right, but we have got some more things that I think we can do better.

We have a good panel with us here today.

I assume Mr. Lewis is joining us shortly? Nobody seems to know.

Mr. Lewis is not here yet? All right.

He will go last. But we will have him here shortly.

We have James Andrew Lewis, who is director and senior fellow for technology and public policy programs—let us get the titles here right; David Lehman, senior vice president and general manager, Command and Control Center at The MITRE Corporation; Dr.

Brian Cohen, Institute of Defense Analysis; and Dr. Stuart Starr, the Center for Technology and National Security Policy at the National Defense University (NDU).

And I want to thank you very much. NDU has been enormously helpful in my efforts over the last few years.

And with that, I will turn it over to the ranking member on the committee, Mr. Thornberry, for any opening comments he may have.

STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. THORNBERRY. Thank you, Mr. Chairman. And I want to join you in welcoming our witnesses on this important topic.

The globalization of the world's market presents a lot of opportunities, but also challenges for us. And how the United States can be innovative enough to protect our national security is something we all struggle with, given some of those globalization challenges.

We have a terrific group of witnesses, and I look forward to hearing from them, as I know you do. And I yield back.

Mr. SMITH. Thank you, Mac.

We will start with Mr. Lehman.

STATEMENT OF DAVID H. LEHMAN, SENIOR VICE PRESIDENT AND GENERAL MANAGER, COMMAND AND CONTROL CENTER, THE MITRE CORPORATION

Mr. LEHMAN. Mr. Chairman and honorable members, thank you for the opportunity to appear before your committee.

My name is David Lehman. I am a senior vice president at The MITRE Corporation. I am also general manager of MITRE's Command and Control Center, which is a part of the Department of Defense's command and control, communications, intelligence, federally funded research and development center. Also, I was MITRE's chief technology officer for nine years, managing our internal research program.

I would ask that my prepared statement be included in the record.

Steve Jobs of Apple said, "An innovation is an idea that ships." The idea may start as a technical curiosity, a result of scientific research. If someone connects that curiosity to a solution to a real-world problem, an invention is created. If people or organizations adopt that invention, an innovation is created.

Too often, the research community lacks an understanding of real-world problems, and the potential users do not know that the enabling technologies exist. The result is too few inventions and even less innovation.

To combat this, we must create an environment and process that carry research results through invention to widespread adoption. This will result in innovation.

In my testimony today, I will present three recommendations to improve the processes and the environment to increase the yield of innovation from our science and technology community. I will focus less on research—the creation of technical ideas—and more on the management process necessary to increase invention and innovation.

These recommendations are: align S&T investment with warrior needs and improve the funding mechanism to carry research inventions through to innovations; adopt open systems architectures for program of record, so that these programs can more easily accept and adapt innovations; and, three, change the business model used in programs of record to increase incentives for contractors.

The key to a good research program is to align investments with the goals of the organization or the needs of the end user. When an organization fails to achieve such alignment, the researchers tell the developers, "You do not use anything we invent," and the developers retort, "You do not produce anything we can use."

This standoff occurs, because the two departments have not worked closely together to understand the needs of the customers or the organization, the research problems, the research risks and the funding profile that links the research schedule and budget to the production schedule and budget.

When an organization can solve these problems, it can put a plan in place that includes continuous dialogue and adjust the plan as necessary over time. Optimally, this process bridges the chasm between research and production.

I should caution that the linkage among the customer, the researcher and the developer should not be too tight. This only achieves incremental improvements, not disruptive, quantum leaps. A good research program balances this tension.

Government organizations have proven that they can achieve optimal alignment between research and development. The National Reconnaissance Office (NRO), in the 1970's and early 1980's, tightly linked its research investments in increased sensor sensitivity and satellite technology to production projects. This resulted in continuously improved intelligence collection capability.

The NRO could achieve this alignment of budgets and schedules partly because the users, the programs, the developers and the research organization all reported to the same manager, creating unanimity of purpose and control.

Then NRO also had exceptionally strong and technically competent program officers. They were essentially the technical peers of their contractors.

Beyond organizational structure and technically strong program officers, there are four additional reasons why most organizations do not achieve this alignment. Currently, neither the research community nor the acquisition community fully understands the needs of the end user. And here we are talking about the warrior.

The well-intentioned but overly bureaucratic documentation review process isolates the warriors from those who will design and build the system. The formal research and acquisition process, as practiced, offers too few opportunities for rich dialogue between the engineers, who know what technology can do, but do not understand the warrior's problems, and the warriors who have the experience, but not the technological insight.

This dialogue, which links the technical curiosity or idea to the real-world need, leads to problem discovery, invention and innovation.

To achieve this kind of interaction in the research and development cycle, we need to create a development environment in which the warriors and the technologists interact continuously, experimenting with new inventions and applications and rapidly incorporating those that prove themselves into the programs of record.

Such a system would combine with what the acquisition process does best—training and sustainment—with what develop-in-the-field does best—satisfy the users' requirements.

Second, the S&T community's research portfolio is not well aligned with both the needs of the warriors and the program of records that exist to satisfy those needs. Tighter alignment must come from joint management of the investment through continuous dialogue among warriors, research and developers. Otherwise, we will continue the pattern of research results that are never used, and programs that are less technically advanced than they could be.

Please note, only part of the S&T budget should be tied to users' needs in existing programs of record. The S&T budget is a portfolio, some of which must be invested in disruptive advances.

Third, research schedules are not aligned with acquisition schedules. Achieving such alignment is understandably difficult, because research does not follow a schedule. Government programs must learn to manage the inevitable uncertainty.

Service laboratories regularly present inventions to acquisition programs, but the acquisition program usually has little latitude to make changes. The acquisition process can manage the uncertainty with advanced, collaborative planning between the program and research communities and continued communication throughout the research and development cycle.

The fourth failure in alignment relates to funding. The research and acquisition communities must plan for success from the moment they embark on a research project. The funding profile in the program objective memorandum must bridge from research funding through acquisition funding.

Too often, research programs, advanced concept technology demonstrations, joint expeditionary force experiments, and the like, validate operational needs, but the budget lacks funding for follow-on development, acquisition and fielding.

To deal with this uncertainty, the acquisition community needs to have a set of funds available that allow it to harvest the best ideas that have achieved practicable results. In economics, this approach is called "real options."

Having a line in the Program Objective Memorandum (POM) that gives program managers the flexibility to apply funds to research investments, as they mature, and carry them into programs of record will increase the innovation yield from the S&T community.

This line item should be large enough to harvest some, but not all, successes, forcing services and programs to prioritize user needs and control budgets.

As a corollary to this observation, we must improve our ability to manage failure. If we recognize and deal with failure early, we can afford more new starts. That is my second recommendation.

Once programs have achieved alignment, they must ensure that the systems they field are designed with open architectures. They must have defined interfaces and use well-known and accessible commercial standards.

A good architecture allows a system to be modified easily, and thus accept with relative ease some—though, unfortunately, not all—future innovations and improvements. Google, eBay and Amazon do this very well.

The Department of Defense (DOD) acquisition community is striving to build systems with open architectures. To meet this goal, the DOD must find a new business model for its contractors. And that is my third recommendation.

Under the standard model, the DOD lets a contract for an entire system, usually for its entire lifecycle. This gives the contractor little incentive to design an open system.

The DOD should let a contract for a base infrastructure with as open a design as possible, then let separate, smaller contracts for the applications that will ride on the infrastructure, and bar the infrastructure contract from bidding on these applications.

The contracting community will undoubtedly find it difficult to adapt to this change; however, such a structure is vital. It will allow the DOD to become a faster adopter and beneficiary of innovations.

In summary, to increase the yield from our S&T investment, I recommend that the DOD strongly encourage the S&T community, the acquisition community and the warriors to manage the process as a team. They must be in constant dialogue to determine needs, create investment and align budget schedules, architectures and acquisition strategy.

All this will maximize the impact of S&T procurement dollars for the warrior.

The DOD already possesses the authority to act upon most of these recommendations. What is needed is some flexibility in the POM line.

Finally, I would like to mention the possible contribution of Federally Funded Research and Development Centers (FFRDCs) in the context of these recommendations. FFRDCs could play key roles, because of their combination of technical expertise and their inherent, government-mandated impartiality. They are honest brokers.

This impartiality is especially important, because commercial organizations can freely share their latest proprietary findings with FFRDC staff. And, because FFRDCs have no commitment to a particular vendor or system, FFRDCs can augment expertise of government program offices, to scan all sources of innovation and objectively evaluate technical innovations against measurable criteria.

I believe that implementing the recommendations outlined above will keep the United States at the forefront of applied technological innovation and contribute to the success and safety of our warriors.

Thank you, Mr. Chairman. I would be happy to answer questions.

[The prepared statement of Mr. Lehman can be found in the Appendix on page 39.]

Mr. SMITH. Thank you.

Mr. Lewis.

STATEMENT OF JAMES ANDREW LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAMS, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you, Mr. Chairman, and let me apologize for being a moment or two late.

I would like to thank the committee for this opportunity to testify. I am going to make four points in my testimony that I will summarize for you now.

First, as you know, technological leadership has contributed to U.S. military superiority and economic strength for almost 70 years.

Second, globalization and other changes means that the U.S. share of innovation and its technological leadership will decline.

Third, some U.S. policies reinforce this decline. These policies include underinvestment in science, a more difficult regulatory regime and the unintended effects of some regulations put in place since September 11th.

Fourth, while the U.S. faces challenges when it comes to technological leadership, it also has an opportunity to respond in ways that can advance its security.

The key to technological leadership is innovation. This is an overused word, but it is the ability to use knowledge to create new goods or services.

The U.S. has been a world leader in innovation. Our political and social makeup provide it with an advantage over other nations. The question is whether this comparative advantage is enough in an era of heightened global competition.

Now, I should note, Mr. Chairman, that there is an anomaly in these concerns. And that anomaly is that the U.S. spends more than any other nation on science and on research and development. And it is reasonable to ask, if we spend so much, how can there be a problem?

The answer to that, I think, is we are not spending enough to maintain our lead, and we are not spending enough on the things needed for military technology. Our spending levels are flat. Spending in other nations is increasing.

If these trends continue, the long-term result will be the U.S. will no longer have the lead in important military technologies.

The issue is complicated, because the results of underinvestment can take years to appear. It is also complicated, because the data is ambiguous.

It is hard to measure innovation, so the normal practice is to use proxies, like the number of patents awarded, the numbers of Ph.D.s and engineers, or the number of scholarly articles published by scientists.

When we look at this data, it is not clear that the U.S. is losing ground. But there are troubling trends. In a few key areas, scientists in other nations are publishing more than their American counterparts.

In our technological workforce, we are coming up to a period where many engineers and scientists will be of retirement age, and they will not be replaced.

From an economic standpoint, this may not be bad. We do not want to train engineers, only to find there are no jobs for them.

But from a national security perspective, these are important warning signs. We should not ignore these warning signs, because they reflect significant changes in the international environment. These changes will challenge U.S. leadership.

One change, as you know, comes from globalization. Globalization diffuses technology around the world. It has eroded the national character of science, because research is increasingly carried out by multinational teams.

Another challenge comes from the rise of strategic competitors. Nations like China or India, or perhaps in the distant future places like Brazil or even Europe.

These challengers have seen how important science has been to U.S. military leadership, and they are copying us.

A related challenge comes from Asia's economic ascent. The Pacific Rim is the focus of global activity. The U.S. is part of this, but the most dynamic growth has been in Japan, Korea, Taiwan and now China.

Asian nations hope to repeat the success they have had in manufacturing in scientific research. If today, Asia is the world's factory, its leaders hope that tomorrow it will also be the world's laboratory.

Another challenge, and a broader challenge, comes from the way societies create wealth. In the 1800's, the U.S. transitioned from agriculture to manufacturing. That meant that the best way to generate wealth lay in industry, not in farming.

Now we are transitioning from manufacturing to the creation of information and knowledge and services. This transition may be good for the U.S. economy, but it has serious implications for military technology.

The cumulative effect is a new kind of risk for national security. The best way to describe this risk is that the vigorous research and technological base that has given the U.S. a military advantage for decades is in danger of being eroded.

Congress can play a key role in stemming this erosion. The most important step is funding for research.

While the U.S. continues to lead in many research areas, it is not spending enough to sustain this lead. U.S. spending in scientific areas that are key to national security is flat or declining, while other nations are accelerating their spending.

These effect of underinvestment is damaging in physics, aeronautics, mathematics, computer sciences and engineering. Research in these areas provides the basis for military transformation, and in relative terms, these areas have been the most seriously underfunded.

Underfunding is compounded by changes in the nature of research and development in the Department of Defense and in the private sector. Government and industry now have to spend more on development, rather than on coming up with new capabilities.

These changing priorities mean that some key research areas are no longer funded.

U.S. policies on immigration and technology transfer also damage technological leadership. This is an area where the Congress could provide assistance.

U.S. national security and military power was strengthened in the 20th century by an influx of foreign scientists. The universities and institutions that received these scientists became global leaders.

But the U.S. is a less attractive destination for scientific talent than it once was. Measures imposed since September 11th have the unintended consequence of deterring researchers from coming to the U.S.

Other changes prevent researchers from staying here once they complete their education. Our universities produce great researches, and then we force them to leave.

Restrictions on technology transfer also work against U.S. leadership. There are some restrictions that affect how scientists can work. There are other restrictions that encourage other nations to invest in their own research and technologies.

The unintended effect of these restrictions, combined with the restrictions on immigration, is to move science outside of the United States. The U.S. is essentially creating its own competitors.

This situation is troubling, Mr. Chairman, but it is not irreparable. And let me tell you two stories to show this.

In 1957, after the Soviet Union launched Sputnik, President Eisenhower's science adviser predicted that, because of their lead in math and science education, the Soviets would surpass the United States in 10 years. He was wrong.

In the 1980's, many pundits said that Japan's rapid growth and its trade policies and manufacturing skills would make them the leading economic power within a few years. They were also wrong.

Now we hear similar predictions about China and India. In thinking about these predictions, it is useful to ask why the Soviets or the Japanese did not succeed. Some of this has to do with weaknesses found in those countries. Every nation has its own strengths and weaknesses. And the U.S., as I mentioned earlier, has some unique advantages.

A more important factor lies in the U.S. response. In each case, in the 1950's and the 1960's and the 1980's, the U.S. changed its policies and practices. The lessons from this is that, if the U.S. finds the right set of responses, the problems it faces today are imminently manageable.

There has already been some progress. There has been a number of eminent commissions. There have been reports. The President announced his American competitive initiative, the Competitiveness Initiative, and both parties have put forward programs for strengthening innovation.

But these are only initial steps. There is still much to do.

As the committee contemplates what to do next in harnessing technology for national security, I would like to conclude with four general recommendations.

First, make the promotion of innovation a goal for policy law. This may require streamlining and simplifying the regulatory burden on innovators.

Second, identify where government action can be effective. One area is funding for basic research in the physical sciences. Without government support, the U.S. lead in these sciences will decline.

Third, look for ways to expand our comparative advantage. We have a competitive market economy, and that gives us a superiority over some other countries. Policies that reinforce markets and competition will help.

Additionally, measures that strengthen institutions like the Defense Advanced Research Projects Agency (DARPA), the service labs, the National Science Foundation (NSF) or the National Institutes of Health (NIH) and the graduate research programs at our universities will be crucial for maintaining American power.

Fourth, the U.S. should look for ways to expand international cooperation. We have benefited greatly from globalization, and closer cooperation with allies will improve national security.

In conclusion, Mr. Chairman, we face challenges when it comes to technology and national security. But I am guardedly optimistic that we can overcome them.

I thank the committee for the opportunity to testify, and ask that my full remarks be submitted for the record.

[The prepared statement of Mr. Lewis can be found in the Appendix on page 45.]

Mr. SMITH. Thank you. We will do that with the full remarks.

Dr. Cohen.

STATEMENT OF DR. BRIAN S. COHEN, INSTITUTE FOR DEFENSE ANALYSES

Dr. COHEN. Mr. Chairman and distinguished members of the subcommittee, I am pleased to appear before you on behalf of the Institute for Defense Analyses, IDA, which is a federally funded research and development (R&D) center, whose sole mission is to support the Office of the Secretary of Defense and DOD on matters of national security.

The topic of my discussion is on the globalization trends in the integrated circuit industrial base. My recent work has been focused on understanding and addressing concerns about the integrated circuit industry, and in particular on the Trusted Foundry Program.

This program, while not necessarily a general solution, has been markedly successful. The Trusted Foundry Program has been well utilized from the start, providing secure and affordable, state-of-the-art, domestic semiconductor manufacturing services for custom-designed integrated circuits for a wide range of defense and national security applications.

I have submitted a detailed statement for the record. And I would be happy at this point to answer any questions the subcommittee may have.

Thank you.

[The prepared statement of Dr. Cohen can be found in the Appendix on page 51.]

Mr. SMITH. Thank you very much.

Dr. Starr.

STATEMENT OF DR. STUART H. STARR, CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY, NATIONAL DEFENSE UNIVERSITY

Dr. STARR. Mr. Chairman, distinguished committee members, ladies and gentlemen, I am very pleased to have the opportunity today to address this subcommittee on the important topic of actions to enhance the use of commercial information technology in DOD systems.

I have more extensive remarks, and, of course, I would like to submit them for the record.

In my remarks, I try to set the tone, the stage for this activity. But most of my colleagues who have been testifying have already done that well, so I will go ahead and pass on that.

What we have been doing at the Center for Technology and National Security Policy (CTNSP) is looking at this issue over the last four years. To that end, we have done over 40 different studies.

We try to take advantage of the best knowledge from government, industry, academia and think tanks. And from that we have distilled six key obstacles, and we have tried to suggest a set of recommendations that could be derived to deal with those obstacles.

What I would like to do is submit for the record a more formal characterization of the studies that we performed and our synthesis of them into a characterization of the problem and potential activities.

I would like to briefly summarize what we see as the key six obstacles that prevent the effective use of commercial Information Technology (IT) in DOD systems.

Basically, they fall in the categories of a non-attractive market, non-transparency, lack of agility, lack of dominance, an isolating market and the challenge associated with primes and lead system integrators.

I would like to very briefly comment on those obstacles so you have a sense about what we have synthesized from our various pieces.

With respect to non-attractive market, one of the initial things that we did was conducted a survey among people who refuse to do work with DOD and people who did work with DOD.

And to give you an example, in the survey, when people spoke of it as a non-attractive market, they said that DOD does not know what it wants, it takes too long to acquire key products and there are too many barriers to the bid process.

DOD had a complementary study. And there they noted that commercial firms are reluctant to enter, due to the fact of intellectual property rights and the question of cost accounting, auditing and oversight responsibilities.

So, all of those factors combined to create a non-attractive market for the small to medium-sized firms that are the most the creative in commercial IT.

The second part of our survey dealt with the question about their ability to understand how to work with DOD. And there, this issue of non-transparency emerged.

The comment was that the process is too difficult, too slow, too confusing and exclusionary. So the net effect is the people we are trying to reach out to find us too distant and too difficult to work with.

The third area is perhaps the most difficult one. It is this issue of non-agility in dealing with organization the size of the Department of Defense.

Typically, you are all familiar with the planning, programming, budgeting and execution system. And people have observed that it takes between 18 and 24 months to transition from S&T into an actual acquisition.

People in the community refer to that as "the valley of death." I mean, a system can be sitting there waiting for transition, but is unable to begin to bridge that gap. That is an issue we have to begin to attack rapidly and effectively.

The fourth issue, of course, is one that was alluded to by several of the other presenters: the non-dominance of the DOD.

If we look back to the 1960's, DOD was calling the shots as the dominant player. That is clearly not the case anymore.

And, in fact, when we have been dealing with many venture capitalists, they threaten to pull their money out of these small and medium-sized companies, if they, in fact, deal with DOD. So, this is an issue that has to be dealt with.

The fifth issue is this question of an isolating market. If you go to the DOD labs, they will have a mantra which says, "adopt, adapt and develop."

And the idea of adopt is, take a commercial product and use it effectively. Adapt is go ahead and bring in some of the attributes one needs. And then finally, if all else fails, develop.

What we have been finding all too often is that people neither adopt or adapt, that they immediately jump to develop. And so, they are missing enormous opportunities that they should be exploiting.

The last barrier that we find is in this issue of the prime and the lead system integrator. What we are finding there as we have done various case studies is that many of them prefer internal technology and may have conflicting objects about commercial, off-the-shelf products. And they are concerned about time limits and complexity of external technology.

So, in many ways, they are not amenable to taking these kinds of activities and risks on, even though they offer extraordinary opportunities.

Now, the question is, in light of these barriers, what are the options that we have to begin to address them?

Well, a colleague of mine likes to say that, for every complex problem there is a simple, eloquent solution that is wrong. And so, in our view, one is going to have to go ahead and look at a complex set of these activities and balance them off in an intelligent way.

And we have identified basically six steps, and we think that the challenge for the committee is to think about identifying and supporting the right six in a balance that begins to make sense.

And these six step solutions deal with enhancing communications in organizations; increasing resource flexibility; reducing the acquisition barriers that I just alluded to; promoting cultural change; creating a system-of-systems engineering and integration organization and enhancing testing; and finally, adopting requirements for specific missions.

What I would like to do is very briefly amplify on each of those solutions, so you have a sense about where our studies have taken us.

The first one was enhancing communications and organization. And one of the things that we have been finding is this barrier between the Department of Defense and these small and medium-sized companies. And we have a number of initiatives that we think would begin to bridge that chasm.

First, we have extraordinary opportunity with Web portals and the kind of technology that we use every day to enhance the communication between those communities. And we have looked at prototypes we believe that can make a major difference in bridging that gap.

Another key point, you will remember, is that when we dealt with these small companies, they found out that the system was too complicated, too opaque. And so, what we recommend is the creation of tech prospectors and acquisition guides, who can go ahead and understand the needs of the DOD, appreciate the technology and communicate effectively with these companies.

It is too much to ask these small, austere organizations to begin to do all those things unto themselves.

Now, we believe there is an extraordinary initiative that has begun at Joint Forces Command (JFCOM), and this is the Office of Research and Technology Applications, which would be getting to go ahead and systematically deal with those issues. And we believe that they can add a great deal more with adequate resources and authorities.

The second question and second potential solution is increasing resource flexibility. And one of the areas that our colleagues have worked closely with have been the Defense Security Cooperation Agency, the DSCA, as a model. And there is a case where DSCA is used a middleman, where it has resources and it ties into organizations that are best equipped to go ahead and do the acquisitions.

So, we would argue not to create a new acquisition group, but to go ahead and take advantage of existing models and exploit them effectively.

One of the thoughts that we have here is that a joint task force could be set up, led by the Joint Chiefs of Staff, that would work closely with the combatant commands. And our sense is, if they had a fund for prompt procurements to deal with the “valley of death” that we were alluding to, that it can make an enormous difference in transitioning things from good science and technology into products that the warfighter could actually use.

The next area was this question of removing barriers. As we alluded to, small and medium-sized companies are very concerned about intellectual property rights, about the complexity of the acquisition process and the need for other transactional authority.

We argue that a proper mix of those three can go ahead and make them much more effective in responding to the issues that we have begun to pose.

The fourth issue is probably the most challenging. I am sure all of you remember the edict from Machiavelli, that nothing is more difficult than changing the culture of a complex organization. And certainly, we have that problem with the Department of Defense.

So, we believe that the essence of cultural change is education, that organizations like the Defense Acquisition University and organizations like Industrial College of the Armed Forces (ICAF), over at the National Defense University, are the place to turn to, to begin to get some of the necessary educational change to promote the cultural modifications that people need.

Typically, you have got to work with the program managers and the Lead Systems Integrators (LSIs) to go ahead and give them incentives to use commercial technology and adopt Government Accountability Office (GAO)-recommended best practices to go ahead and implement them.

The fifth recommendation we had dealt with the creation of a systems-to-systems engineering and integration organization. And this is one of the issues that one faces, because when one develops these activities, they are not deployed in isolation. They are part of a complex system of systems.

And one needs an architectural vision. As David indicated, ones needs an open system architecture to begin to integrate those capabilities in. What we would like to see is an organization created, so we could begin to test things at a systems level, so one would have an appreciation of whether people's promises are actually realized.

In addition, we would like to see another comment that David made about looking at things in a mission context to understand the contribution that new systems would make to overall mission effectiveness. So, we believe an organization that dealt with that would begin to deal with that problem.

Our last solution was really dealing with particular mission requirements. And one of the areas that we are very sensitive to and have been looking at very carefully over at CTNSP, is the question of using commercial IT to support stability operations.

And what I would like to do is enter into the record a recent study that we did called "I-Power: The Information Revolution and Stability Operations." And we argue that, if commercial IT is used there effectively, it could have tremendous leverage in going ahead and dealing with all the other problems that one faces in stability and reconstruction, to provide a basis for dealing with medical needs, education needs—all of the infrastructures that people require.

[The information referred to can be found in the Appendix on page 71.]

Dr. STARR. So, commercial IT is the key point of leverage that one would begin to use.

Let me complete my remarks by just observing one or two other things that we are doing at NDU that are germane.

We are embarking on a theory of cyber power. And one of the things we are trying to do is to establish a framework to see how the cyber infrastructure, if enhanced effectively, can enhance the levers of power for the United States and go ahead and empower us against adversaries like transnational criminals, terrorists, potential peer individuals.

We believe that one needs this macro framework to begin to look at issues of policy, legal issues, et cetera, to go ahead and make intelligent decisions.

One of the most important issues is the question of the Internet. We have been using that to great advantage, but we are deeply concerned about its security deficiencies.

And so, one of the things that we emphasize strongly is to pursue the activities at the National Science Foundation and DARPA, to go ahead and re-imagine the Internet, in a way, that would begin to fundamentally deal with those security issues, so we would have a firm foundation to build on.

Currently, we see it as a foundation of sand. And we need to go ahead and to buttress that capability.

The last comment I would like to make deals with a recent study that was done at NDU on "The Science and Technology Innovation Conundrum," and I would like to enter this into the record, as well.

[The information referred to is retained in the committee files and can be viewed upon request.]

Dr. STARR. My colleague, Tim Coffey, who is the former head of Naval Research Laboratory (NRL), has observed that there are two key aspects of S&T. One is prospecting, and the other is mining.

In prospecting, one can go ahead and do basic research, and there are issues about the long-term payback. In mining, one gets immediate gratification.

Tim's argument is that we have a major void in governance in the prospecting phase. And that is a major challenge for the government to go ahead and take a strong role there to provide that particular foundation.

I hope these recommendations are of value to you, and I truly look forward to answering any questions you might pose.

[The prepared statement of Dr. Starr can be found in the Appendix on page 58.]

Mr. SMITH. Thank you all very much.

We have just a few members here, so I think we will be a little flexible on the five-minute rule. We will try to keep it close to five or six minutes, but if members have questions beyond that, we will not be too much of a stickler for details on that.

If I could start—actually, Mr. Lewis, your comments about our inability—just lack of funding, certainly, for innovation. I am curious exactly where we need to spend more money, and definitely agree with you.

But then also, the second piece of it, which is, in a post-9/11 world, we are not doing as well at attracting the technologists and innovators to come.

I mean, an enormous advantage that this country had, that I think people underestimate is, throughout the 1960's, 1970's, 1980's and into the 1990's, the smartest people in the world, almost universally wanted to come here. And we, by and large, let them, and benefited greatly from that.

Now, we are a little bit more concerned about the process of letting people into this country. And I understand that, but I definitely think there is a downside we need to highlight more.

So, a second question for you is, how can we change that process a little bit, keeping in mind the security needs? I think we can all agree we have gone too far in the other direction.

The final point, you mentioned some of the controls on exports. And this is really just an observation to put into the record for me. I battled the export control issue on this committee for a long time.

The first time it came up—and this, I believe, was dealing with the encryption piece—I was, you know, I lost the vote in the amendment 46 to 1 in the committee, because the mindset is, we have to protect all of the technology and innovation we have developed here. We cannot let it slip out into the rest of the world, lest they figure out something and it falls into the hands of our enemies.

So, they viewed it as sort of defense versus business. And I have always disagreed with. And you made the point very well.

If the U.S. companies are the leaders in technology in the world, then they are going to put us in a better position to defend ourselves. If we lose that leadership, if it drifts overseas, then we have totally lost any control we have.

So, you know, it is sort of the more we tighten our grip, the more it slips through our fingers kind of thing. And I just wish we could grasp that point.

And as we are making it more and more difficult for domestic U.S. technology companies to export what they do, they ship the innovation overseas and we lose it, and our national security drifts backwards, not forwards—a debate we will have further on this committee, I am sure.

You can comment on that, if you like. But I am curious about the first two parts of the question.

Where can we spend more money? And how can we make some adjustments to get the best and the brightest to start coming here again?

Mr. LEWIS. Great questions, Mr. Chairman. Let me try and answer them.

And let me mention that the points you made on export controls reinforce some of the issues we have on research and on immigration, because American companies will say we are in a worldwide competition for brains.

There are brains, and we would rather have them than our competitors. And if that means we have to go to China or to India or to Europe to set up our research centers to get those brains, that is what we will do. Because if they do not, their competitors will. So you have put your finger on it.

The place I would look for a change in the future is in our aerospace industry, which might be suffering some erosion, because of export controls. So, a serious problem for defense.

On the post-September 11 restrictions, one of the things that has happened is that other countries have gone out of their way. They have looked at what the U.S. did. They love it. They want to copy it. And they are competing with us.

And so, you see, for example, the British had big signs in a Middle Eastern country on the way to the airport.

“Can’t get a visa to study in the U.S.? Call the British consulate.”

The Chinese have awards now they call the "sea turtles"—which I guess is some Chinese pun for sea turtles—returning Chinese scientists, who come from Silicon Valley, bring not only their technical skills, but their management skills. And they get funding, they get housing allowances. They get government recognition. Singapore is famous for this, Australia—the list goes on and on.

To compensate for this, we have to remember that the most important factor is, our universities are still strong. And this relates to the basic research question. If we have strong universities, people will come here to study.

An easy change would be to say, once they study, once they get their doctorate, once they are at the peak of their educational skills, we should let them stay. Our current policy is to make them leave.

Mr. SMITH. And that is something that we, you know, on the immigration debate, that is a piece that a number of us are talking about putting in; if you get that degree, you get an automatic work visa, basically, if you have those skills, you know.

We spend all the money in our university system to educate them, and then we tell them to leave.

Mr. LEWIS. It is interesting to me that other countries are considering a similar approach. If you come in with an advanced degree, they will accelerate your residency permit, or they will give you automatic residency status.

So, we may not have recognized that we are in this competition for brains as a country, but other countries have recognized it. And there are some things we could do.

This is just a tiny slice of the immigration debate. We are not talking about millions of people. We are talking about a high end of students who are getting very advanced degrees, and how do we get them to stay here.

We have innate advantages. They came here for a reason. How do we get them to stay? And changing our rules to accommodate that would help.

Related to that is the question, I think, of basic research.

Funding for basic research is not something that companies will do. They cannot afford it, because basic research does not result in a product that you can sell, right. Or if it does result in something, it is usually open to your competitors.

So, this is an area where the government plays an absolutely crucial role. And it has been an area of strength for the U.S. in the past, because of DARPA, NSF, some of the other activities.

We have made two fundamental problems. We have made two fundamental errors.

The first is, we have kind of rested on our laurels. And so, if you look at the spending—and I know it is a tight budget environment. It is very difficult to argue for more money. And I usually tell the scientists, do not go in and ask for money right away, because, you know, no one is going to be happy.

But our spending has been flat; other countries are ramping up. Particularly flat in areas that I think relate to military technologies, whether that is aeronautics, IT, physics, chemistry, engineering.

You know that about a decade ago, the Congress decided to double investment at NIH, and that has had very powerful results for the American economy.

But the speaker at the time has even said that perhaps it was an oversight not to, at the same time, double funding for NSF, because we have weakened the base of basic research on which so many of these other activities rest. So, I would look for ways to increase the funding there.

I did look at the numbers, Mr. Chairman, since I thought someone might ask that. And there has been a small increase in the last year. It is a little less than two percent.

When you think about it, that is nice, two percent. But gross domestic product (GDP) increased about 3.2 percent, and inflation increased a little more than 3 percent. So, in effect, a two percent increase is really a cut.

So, my argument would be, in the areas of military significance, increase the funding for basic research.

Mr. SMITH. Thanks.

Mr. Thornberry.

Mr. THORNBERRY. Thank you, Mr. Chairman.

I guess I want to step back for just a second. It seems to me there are two broad categories of issues. One is spending, how much and on what. And the other is processes, how it is to deal with the Federal Government.

And I think nearly all of you, if not all of you, have dealt with that in some way or another, Dr. Cohen by way of a positive example in his written testimony.

I guess I would just like just to go down the line briefly and ask each of you: How much more could we get out of the money we spend, if we improve our processes, if we make it easier to deal with the Federal Government and harvest some of that small, middle-sized companies who are the innovative leaders in IT? But I suspect it is true across the board, too.

So, Dr. Starr, let me just start with you. And if you do not mind, let us just go down the row on it.

Mr. SMITH. If I could just place an emphasis on the “briefly.” If we get a five-minute answer from each of you, that is going to leave some folks behind here, so let us shoot for a minute, minute-and-a-half, thereabouts.

Go ahead.

Dr. STARR. Okay. That is really a brilliant question. And I think process is vital.

As one example, I have worked with the Defense Venture Catalyst Initiative—DeVenCI—that OSD did. And it went ahead and used venture capitalists as a way of identifying where there were interesting capabilities and leading these people through so they could be more effective.

The challenge of those efforts is that they are too little too late. And so what we need is to begin to expand those on a large enough scale to reach out commensurate with the nature of the problem.

So, I agree with you completely, that we need new processes. We need these tech prospectors, we need acquisition guides, but we need enough of them to make a difference in the problem.

Mr. THORNBERRY. And my question is, how much is that going to help? I mean, a lot? Could we get a whole lot more bang for our buck, if it were easier to deal with the Department of Defense?

Dr. STARR. Yes. I believe there is an extraordinary payoff, not only in terms of intellectual tie-in, but in addition, if one had brought technology to bear in terms of Web portals and made it much more transparent for people to understand what is going on.

I mean, the barriers that I spoke about were the questions of opacity, complexity and things of that nature. It could make a big difference.

Mr. SMITH. If I could interrupt, just as we go down the line. I think that the big thing to focus on here, when you talk about the process—you know, why is it so cumbersome, why is it such a problem—there is kind of an implicit assumption that it is just, "Eh, bureaucracies, that is the way they are." And that is not really true.

To my mind, the biggest reason that all of this is in place is, we are talking about a lot of money. And everybody wants to make sure that, when that money is spent, and if anything goes haywire, they can say, well, you know, we did the 55 forms, and we bid this through the 6 different companies, we crossed all the T's and dotted all the I's about 5 different times. And even though everything went haywire, hey, we did what we could.

And so, if we are going to do this and fix this, we have to be willing to take a little bit of a risk, which I personally am willing to take, to say we are going to empower decision-makers at every step along this process to say, you know, assistant whatever for procurement, you get to decide.

Is this the right thing? Buy it. We are not going to make you fill out forms and go up four levels of command.

As you answer this question, if you could touch on that tradeoff between protecting against that and the way it bogs us down, I think that would be helpful. If we can go down the line, is fine.

Dr. COHEN. Let me offer my personal opinion. The idea that once defense dominated industries, have now become commercially dominated, yet we could still use the same processes that we had in the past, really has to come under close examination.

I think, my work with the Trusted Foundry has made clear to me that, actually, new approaches, whether they be business structures, ways of partnering with commercial industry, offer significant opportunities for innovation.

As Dr. Starr had noted, while the Department has traditionally developed things very well, they have not always adopted them. And our ability to use commercial technologies and get them quickly into practice is really hindered by the processes that we have in place.

So, I would speculate that there would be significant advantages in innovating in those sorts of business practices and processes to allow you to take commercial technologies, partner with these commercial industries, protect the intellectual property that is at the heart of the profit-making in commercial industries, but at the same time accelerate getting those technologies into place for the Department at much lower cost.

Thanks.

Mr. LEHMAN. I would agree that I think we can get a lot more out of some new processes here. I think one of the examples is, In-Q-Tel has done a very good job of—and they have gotten the users together with the venture capitalists very early on in this process and said, you know, if you do this to the product, there is a market for it, and we will supply that market.

And it has ended up that they have had to invest much less in these companies than they originally thought they would have, because the venture capitalists like the fact that they are bringing a market, and they do not really want the government to have equity stake in the company, because that is less for them. But they are willing to put more money in it themselves, because the government has said that there is a market here.

So, I thought that was a very innovative approach and is showing the kinds of results that you can get if you do that.

In my prepared statement, I had an anecdote in there from iRobot, which is a small company. You may have seen the Roomba vacuum cleaner. But they also make a PackBot, a robot, which the DOD uses for exploring caves, and the like, in Afghanistan.

They had to hire a retired admiral to help them through the acquisition process and the mire of regulations. And so, if we can lift those regulations, it will make it a lot easier for other companies to do, as iRobot did, bridge that gap from small business innovative research (SBIR)s into real products.

Mr. LEWIS. You know, it is a great question, and I think all the points have been useful.

If you remember CORONA, which was our first spy satellite, CORONA was finally launched after 13 successive failures. So, I wonder if we could ever have a program like that again, where the people would be able to—yet it was a tremendous success.

And so, the point about accepting more risk is crucial. We are more risk-averse and that hurts us.

Streamlining would be great. I do think there would be some bang. I was trying to do some really cheap calculations in my head, so I apologize if they are a bit informal, but this would buy us a few years, maybe five years. But at the end of the day, we are going to have to ante up a bit more.

Mr. SMITH. Thank you all.

Mr. Marshall.

Mr. MARSHALL. Mac, were you finished?

Mr. THORNBERRY. Yes.

Mr. MARSHALL. This is territory that is relatively unfamiliar to me. And I find myself, as I listen to you and glance at your testimony—I have not had an opportunity to read it thoroughly—finding that you are in agreement with one another that we are too cumbersome, too over-regulated, too slow to be as effective as we might be.

And all of you are very familiar with the reasons why we are too slow. And each of you says we ought to lessen the regulatory burdens, lessen the—but you know why we do that. The chairman here kind of described.

Is there reform out there that keeps the baby and tosses the bathwater that you are aware of? Or are people simply at the level of frustration where it is beyond human scale? We really do not understand how we got into the mess that we are in; we just recognize that it is a mess.

It is too complicated, and consequently is slowing us down, costing us lots of opportunities and making it very difficult for us to accomplish our objective at a reasonable expense.

Or is there something specific that we ought to be adopting that you are aware of? Has somebody come up with this is the way we ought to be doing it, it meets the objectives that are served by the current system and it also enables us to do this quicker, more efficiently?

Dr. STARR. Let me take that first. And I think there are some real innovations that are going on that we want to take advantage of and build on.

In my testimony, I alluded to ORTA, the Office of Research and Technology Application that has been created down at Joint Forces Command. And they have gone ahead and signed multiple contracts with various companies to go ahead and share development activities, working SBIR activities, holding fora to explain to small and mid-sized businesses what their needs are.

But the thing is, ORTA is a miniscule activity, just a few people, limited authorities. And so, one point would be to go ahead and build on that activity, to provide them with more prospectors and acquisition guides to begin to expand things.

So, I think that is a useful thing.

Mr. MARSHALL. Let me interrupt.

Dr. STARR. Go right ahead.

Mr. MARSHALL. All right, let us assume that we are not going to begin by changing the entire system and using the model that you just described as the model for the entire system.

What work do you funnel to ORTA that would best—if you are going to expand, how do you expand?

Dr. STARR. Well, I think one of the key points about ORTA is that, Joint Forces Command tries to speak for the combatant commands, so, the user. And so, it has been a good window for them to go ahead and have the combatant commanders explain what their immediate needs are, and to reach out to organizations.

You are right. And again, there is no single, silver bullet that is going to solve all these problems.

Another area that I think is a complementary activity, is just about every service in OSD—and David alluded to In-Q-Tel—has been trying to take advantage of venture capitalists.

And they have done very different models. I mean, almost everybody, in fact, has pursued a slightly different path.

But they are probably underfunded. I think they are doing some very useful work, and they should be working much more cohesively together.

When In-Q-Tel finds something that is not quite useful for them, they should be able to pass it off to the Army or the Navy, or whatever organization is appropriate.

So, I think there is strength in unity there, where the venture capital activity has been very fragmented. And more cohesiveness there could make that a more potent technique.

I certainly agree with you that there is no one mechanism that will resolve all of these issues. But there are a few that have promise, and one can build on and expand.

Mr. MARSHALL. I guess, to any of you, who is working on—who is it that is trying to reform this process in a way that makes sense? And who has come up with some—is anybody doing that? I mean, you have got some suggestions, and then you observe that the rest of it is just——

Mr. SMITH. If I could interrupt just a second.

We are. Our committee is. And I will say that the report that Dr. Starr referenced a few moments ago was as a result of a request from this committee, that I and some others worked with Dr. Starr on.

In last session we then tried to implement some aspects of that report—unsuccessfully, but I am hoping for a more favorable review this time.

And we are going to continue working on that and trying to expand upon what is going on at the Joint Command to try to expand those opportunities. It is one of the big things in the science and technology are that I want to get to.

I want to get to the point where we are empowering the—you know, however the command structure works. If it is the combatant command, you know, the theater, wherever it is, let us empower them to make more decisions so they can cut through the acquisition process.

So, and Dr. Starr.

Dr. STARR. Let me just amplify one point, as well.

You asked, is anybody trying to deal with this. We have, in fact, briefed the chairman of the Joint Chiefs of Staff and key players on the Joint Staff. So, they are working it.

It is just that they have not quite converged on good solutions at this point. They have been interested in what we are saying. They are absorbing it and they are trying initiatives. It is just a question about work in progress.

Mr. MARSHALL. The process of reforming the process is what we are talking about right now. And if the process of reforming the process is as ad hoc as was just described by our chairman and you, then we are missing the boat.

There ought to be a more formal, understood way to tackle what is recognized by all of you gentlemen and us as a problem than this committee trying to drive it with the limited lights we possess.

Mr. SMITH. No offense intended to our staff, I suppose. I do not think we are quite as limited as that, Jim, but I respect what you are saying.

And one of the challenges that we face, and one of the things that we are working on, is to get the military on board with this. And, you know, they have got a lot to do.

Number one and number two, they do not want to be dragged too far down a road that they are left holding the bag on, which I respect. But we are working with them to try to get to that point.

Mr. MARSHALL. May I——

Mr. SMITH. Sure.

Mr. MARSHALL [continuing]. Just one more observation about it. I cannot remember the name of the professor, but a couple of guys wrote a book some time ago about businesses that get beyond human scale, and described the challenges those businesses face.

The Pentagon has been beyond human scale for a long time. And we are kidding ourselves if we think this committee and its limited staff is going to be able to solve this problem.

It is processes. You put together a process to attack the process, if you are going to be successful, it seems to me.

And we ought to at least talk a little bit about that, and that is why I asked the questions I asked.

Mr. LEWIS. Can I add something on that, Mr. Chairman?

Mr. SMITH. Certainly.

Mr. LEWIS. Thanks.

I think you are right, because I know that sometimes I have been in meetings where we have talked about doing projects on acquisitions reform. And people run screaming from the room. It is an overwhelming task, and it will take a very long time to untangle this knot.

In the interim, there are a couple of things you can do. The usual approach is to create some new organization outside of the existing dinosaur. And say, the new organization—it is small, it is flexible. Let them try it. If it does not work, it goes away. In-Q-Tel is a good example.

Another one is to find a way to give an organization the power to waive some of the acquisitions requirements, and if it needs to be, an emergency or a crisis or mitigating circumstances.

But those are the two steps that most people use while you confront what is a crucial problem, but a problem that may take awhile to solve.

On a note of consolation, let me say that, when I think about our processes, our processes are very complex. You could even describe them as "bad," but they are less bad than the processes you see in other countries. So, we are still a little bit ahead there.

I do not know if I would want to rest on that one very long, but in the interim, there are intermediary steps we can take to speed things up.

Mr. SMITH. And I am realistic about the challenge here. I do not think you can invent a process that saves you from the problems of process. As the sentence would imply, the process itself can strangle you.

And there is only so much—we are spending a lot of money. And a lot of people are involved in that process, from the warrior right up through the chain of command, to the congressional side of it.

There is no way to sort of peel all those people back and create some seamless, streamlined dictatorship. We have to understand that is the way the system works, but we have to—you know, look for the places, as all of you have done, where we can make some improvements on that.

Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman.

I share your idea about being willing to take greater risks on trusting people to make decisions, but until you and I and our colleagues give up the Monday morning quarterbacking and the, you know, tour the battlefield, shoot the wounded kind of mentality that we live in, where we punish decisions that we do not agree with, where we punish decisions that lead to failures that, in hindsight we would have something different—till we get rid of that mentality, then no one on the uniform side of those tables—you know, they have got a tough job to do.

Because we get to evaluate what happened, and then Monday morning quarterback, say, well, I have would have done it this—now that we know the results of those experiments, I would have done it a whole lot differently in my infinite wisdom.

But I think we all recognize our penchant for that, and it goes with the territory, just part of the system, unfortunately.

Could you gentlemen help me understand? We spend $3 billion at DOD, or $80 billion, I think, somebody's testimony showed, overall, the government.

How do we start with or vet? How do we figure out what we want to research, what we want to look at?

I do not understand, really, how we decide collectively where we want to go. It seems like we have a zillion little places to get to. But is there a board of science and technology research that says we need to focus here, here and here? Or is it just ad hoc, whoever has come up with today's best idea goes at the funders?

How does that system, top-down, look? I mean, how do we apportion our efforts, whether it is dollars or efforts themselves, across that huge spectrum of science and technology and research?

How do we focus? Or do we focus?

Mr. LEHMAN. Well, there are multiple—it is not a single, top-down activity. The Office Director, Defense Research and Engineering (DDR&E) has some responsibility for that. Each of the service labs has some responsibility for that.

And there is a huge requirements process out there that starts out at the combatant commands that rolls up through, and the service labs will respond to the requirements in those documents.

That is a good start. But as I said in my testimony, you miss the rich interaction of the service lab people actually getting out in the field and seeing what the problems are.

And they respond to that, but then they are disconnected from the acquisition programs that are actually going to build those programs.

So, the planning process needs to be——

Mr. CONAWAY. Is this research focused on just the applied research, as opposed to——

Mr. LEHMAN. It is both.

Mr. CONAWAY [continuing]. We do not know what we do not know?

Mr. LEHMAN. It is both. It is both.

Mr. CONAWAY. We ought to have folks out there who are just trying to explore for the sake of exploring.

Mr. LEHMAN. And there are people doing that.

Mr. CONAWAY. So, if everybody is in charge of that, then nobody is in charge of that.

Does the pyramid not shrink to the top, where at least one small group of people says, we need some folks out here thinking about the unthinkable, and we need some other folks thinking this warfighter needs X, a way to defeat improvised explosive devices (IEDs), so you have got it coming from both ways?

Do we have any system like that anywhere?

Mr. LEHMAN. I think there are multiple pyramids. There is not a single pyramid.

Mr. CONAWAY. So then if everybody is in charge, nobody is in charge.

Mr. LEHMAN. Well, it is not everybody, but there are multiple pyramids. There is a pyramid for each service, and there is an Office of the Secretary of Defense (OSD) pyramid.

Mr. CONAWAY. Okay. Thank you, Mr. Chairman.

Dr. STARR. Let me just amplify on that just a bit, because I believe you are going to have John Young giving a presentation here.

And over the years, I have been a member of the Technology Area Review and Assessment Process, whereby there was project reliance and they took the various S&T activities and structured them, and began to make some judgments about how they were doing and where there were important shortfalls.

So, there is, in fact, a formal process that is used. There are questions about it. I know, as a reviewer, I was unhappy with it, because it was incomplete and it did not give us an opportunity to really weigh in the way we thought we should.

But there is a foundation to build on, and you should certainly speak to Mr. Young, and I am sure he can amplify it.

Mr. LEWIS. You also are going to have, I think, Dr. Tether from DARPA. DARPA has a relatively interesting system where they take young researchers, mid-career researchers, bring them in for a few years to manage programs.

These are people who know what is going on in the research community. They have an idea where to spend the money. They hear from DOD what some of the bigger problems are.

And then after four or five years, they leave and go back into the scientific community. That process of refreshment is really helpful in doing the kind of targeting you are talking about. He may have more information on it.

Mr. SMITH. Ms. Gillibrand.

Mrs. GILLIBRAND. Thank you, Mr. Chairman, and thank you for holding this hearing. I think the topics that we are discussing today are of vital importance for our national security and for our economic growth.

In my district—I am in upstate New York—we have begun to focus a model on bringing universities together with the DOD in a very innovative and exciting framework. So we have the State University of New York (SUNY) campus that is doing the Center for Nanotechnology. And almost half of those contracts are DOD contracts.

We also have the Request Progression Interface (RPI) system, and they are doing enormous amounts of innovation.

And from these two areas of learning and education have spurred a number of small business. So I have one small business who has created this ball that a soldier can roll into a war zone, and it has a 360-degree view of what is happening around that corner, to give the soldiers real-time intelligence about what is happening.

Other producers are making a great new material to make stronger vests to protect our soldiers, a material that we are now using on the space shuttle to fix the tiles that come loose. It is impervious to heat and is very strong, but very lightweight.

And so, what I would like to ask you to comment on is, how can we as legislators improve the likelihood of the DOD using this model to its benefit, to center its research around educational facilities and to have those kinds of contracts where you have the benefit of innovation, but you also have the security of having these labs based in the United States, so all this work is not continually outsourced?

I read somewhere that chip manufacturing is continually being outsourced to other countries, and that really creates security concerns for us, because we need them manufactured here. We need to be on top of the intelligence designed here.

And what I would like to know from you, I would like to have guidance on how you think we, as legislators, can improve the regulations, create funding models, perhaps, where we can have these centers of innovation, where they can be surrounded around these university systems where you have the best new ideas coming out, and have the DOD actually be part of those facilities, so that they can build from within and have that technology be in-house?

I have read through your testimony that you have some ideas about public-private partnerships, which I think are strong. But we need to maintain ownership of this technology.

And I do not think just contracting out to the private sector is the solution, because then you have the problem of the current DOD acquisition timelines, that are very, very long—one year, two years, three years out—when you have already come up with a new idea.

So, I really want you to advise our committee on what are some ideas for looking at the most innovative frameworks for innovation and growth and design and new technologies, which I think is the education system hubs that we are doing well in our district, and how that could be used with the DOD.

Dr. STARR. Well, let me make one quick observation.

We have probably the world's expert in the audience here, Dr. Bill Berry, who recently joined National Defense University. And he was deeply involved with overseeing research in the Multidisciplinary University Research Initiative (MURI) program and things of that nature.

So, I am certainly not an expert, but Bill is. And so, perhaps for the record, he could go ahead and respond to your comments.

Mr. SMITH. Yes, that is permitted. And we will just—if you could come forward. And he is a member of the same organization as Dr. Starr.

Just state your name for the record, so we can get that.

Mr. BERRY. I am Bill Berry. I am at the Center for Technology and National Security Policy at the National Defense University.

And the issue you raise, I think is an important issue. I think there are some models that the Defense Department is already using, which establish center-like organizations.

We have a number of different models that are used. There are university-affiliated research centers in various parts of the country.

Another interesting model, I think, is one that the Army Research Lab is using called Collaborative Technology Alliances, where they work directly with the Army Research Laboratory, either at Aberdeen Proving Ground here in Maryland, or in Adelphi, in a number of areas where we bring in work done in the universities, but also in the defense laboratory in this case, and working closely with industry, so that the new ideas that are generated there have a pathway from the university and the laboratory directly to industry.

There are a number of other models, I think, that are not so much regional. But we do have the Multidisciplinary University Research Initiative, which is a center-like program, that generally involves a number of universities across the United States.

And a major effort has been done over the past four or five years to link those institutes with our defense laboratories more closely, so that the products and the ideas that are generated there do feed directly into our laboratory systems, like the Naval Research Lab, the Army Research Lab and the Air Force Research Laboratory.

So, I think a lot is being done in that regard to try and set up these kinds of opportunities for integration across academia to defense laboratories and industry. And I actually think we have done a reasonable job there.

Some of those are regional, as you suggest, in the case of the New York State model you mentioned. But some of them are spread across the United States to take advantage of universities in any state that can contribute in a given area of research.

Mrs. GILLIBRAND. Is there something that we can do legislatively, in terms of regulatory aspects, or in terms of appropriations, that would facilitate that process?

And second, do you think the work that has been done in those kinds of university hub paradigms, is it effective? Is it proving to be effective in the design and creation of new technologies that benefit our soldiers?

Mr. BERRY. My answer to that immediately would be “yes.” I think it is being very effective. And I think any time when you can bring those three communities together—that is, the defense laboratory, which has a lot of unique capabilities that you will not find either in academia or industry and has the ability to work across the domain of classifications—that is a real benefit.

But I can give you examples of lots of things that have come out of these kinds of unions, like control algorithms for autonomous systems that go directly from university ideas for algorithms to control these things, tested in the defense laboratories, and industry picking those up and actually developing them into these autonomous air vehicles, for example. That is one that comes to mind immediately.

I think, things that you have heard here, the need for increases in fundamental research, that is really the stimulus and lays the foundation for all of the things that the Department of Defense is going to use in the future, is an important——

And I always applaud the ideas that we have to increase basic research, primarily in physical sciences in the United States, and people always want to lift up the National Science Foundation and

National Institute of Standards and Technology (NIST) and other places.

But a very large part of the engineering research, in particular, and physical sciences research in this country is actually done by the Department of Defense. And we have not really included increases in basic research in the Department of Defense basic research programs, I think, to the extent that we should.

Mrs. GILLIBRAND. Thank you.

Mr. LEWIS. Let me give you another example, if I could, that would be quick.

One of the states that has been very successful in doing this is, actually, I think, North Dakota. And what I usually say is, if North Dakota can do it, anybody can do it.

But what they have done is focused on their universities as a place where you have got human capital. They have looked for ways to bring in the support you need. And if you need lawyers who know about intellectual property, you need a way to hook into venture capital, these are things the state has to do.

And, you know, there are ways to help state governments think about that.

One thing that is crucial, in addition to increasing the pot of funding that they are going to be competing for, though, is finding a way for these state universities to figure out how to deal with Washington, because, as you have heard from all of us, it is complex. It can be confusing.

The states that have figured this out, like the California system do very well and they are a powerhouse in science.

So, that would be one area you could think about. How do I make it easier for my state to navigate the various channels and pathways you have to get through here?

Mr. SMITH. I think that is, you know—if we did not do anything about the process, and all we did was invested more in innovation and created the atmosphere where the world's innovators could come here and prosper—if that is all we did and did not change the process at all, I think we would make an enormous difference on that alone.

Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman.

And thank you to the witnesses.

I am sorry, as is so often the case here, we have to step out for a bit to attend other committee business. And so, I understand that I missed Mr. Thornberry's question. I just got a thumbnail catchup on it. So I do not want to recover that ground, but I think it will connect to my interest and concerns here.

I am looking, Dr. Starr, at your testimony and I listened with some interest to your recommended actions. You had six of them and they are captured here.

It just kind of makes me want to cry, not because I disagree with the recommendations, but with my own personal experience, I know for almost 20 years, personally, and I know from stories way preceding that, that we have been grappling with almost exactly these same problems and, frankly, many of the same recommendations.

Defense acquisition official, under secretary of defense for acquisition, DDR&E after DDR&E, director of DARPA after director of DARPA has grappled with the same issues.

We have an acquisition system in the Department of Defense that is badly, seriously broken. And everywhere you turn in that process, it seems to me, it is broken.

We have a requirements process. We have to verify requirements in a process that sometimes takes years instead of, arguably, weeks or certainly months.

And as you pointed out, we have, what was it, a valley of death. I forget, one of you pointed out that valley of death.

And so, I am sort of laboring in despair here as I look at these recommendations—"reduce acquisition barriers." That just sort of makes me—as I said, my shoulders are sagging here, because that is an enormous problem.

"Promote cultural change." Everyone, I am sure—and I should never speak for my colleagues, because we are a fairly diverse group here. But I would hazard a guess that we probably would certainly agree with that.

But I do not know that the gentlelady's question, how legislatively we fix that. We are looking for those ideas. You have some expansion here.

But I am just frustrated like all of us. And I know you are, I can tell in your testimony. You are experts in this field and you have been working with them for a long time.

So, let me just focus back to where I think there is a piece here that I am really intrigued by. And that is in your number one recommendation, enhance communications organization, where you say—and I am reading from your testimony—to enhance communications, technology prospectors should be created to conduct more focused searches and facilitate the injection of commercial off-the-shelf (COTS) products into DOD systems.

Absolutely. Web portals should be created to coordinate the use of commercial IT, and acquisition guides should be provided to smaller companies.

And I think that was a part of Mr. Thornberry's question. You have got smaller companies who have great ideas. And how do you get them in there?

And then you mention JFCOM.

But I am sort of open to any of you. If you think in terms of the frustrated entrepreneur out there, or university professor or researcher, who really has this great idea, and you really want to get it in front of somebody, it looks to me like that is what you are suggesting here, is there a way for that—whatever, the round ball that you throw around corners, or speech translators or—there is a lot of good—my district, like others, has lots of small companies that have fabulous ideas.

And I can tell you that it is pushing a rope to get those in front of somebody who is a decision-maker, and, in fact, then, to determine who the decision-maker is, because of all the rest of this stuff—the culture, built-in decades of bureaucracy and process, a testing system that is broken, developmental testing and operational testing. When do you start and where do you start over again?

It is an enormously complicated and, frankly, antiquated and bad system.

I am desperate for a way to wave a legislative, which we could get bipartisan support on, and fix that. I do not know what that is.

But this idea, where would you go to create such a Web portal? From anybody.

Dr. Starr, it is your testimony, so I should go to you.

Dr. STARR. Well, that is a great point. I mean, we see that as potentially one of the contributors to a solution.

In fact, over at CTNSP, one of the initial prototypes we did was create something called Early Military Involvement Speed and Accelerated Results (EMISARS), which was designed—our vision would be that you would have a mall of capabilities and various boutique things that were geared to particular problems of interest.

And EMISARS is meant to be one of the elements that would fit into that mall.

So, at this stage, we have done a prototype activity and worked with JFCOM. It has been stalled, but at least we began to demonstrate—and I note, we share the frustration that you have, obviously. But we think——

Mr. KLINE. I did not mean for that to show on my face so clearly, but I am sorry.

Dr. STARR. But, I mean, it is clear that, in the way we do our normal business these days, I know if I book a trip or if I buy something on eBay or Amazon, et cetera, it is very, very than the way I did things 5 or 10 years ago.

DOD has not kept up.

Mr. KLINE. Exactly.

Dr. STARR. And so, it has to exploit that kind of technology to begin to use it, to take advantage of prototypes and expand their capability to make things more transparent and enhance connectivity.

Mr. KLINE. But one of the things, the ideas that we have been exploring a little bit in this committee through the last couple of Congresses, at least, is the answer to the question: Where does one go with one's good idea?

And we have tried—we have had various testimony. The director of DARPA on a couple of occasions has sort of offered that, well, DARPA is the place that you go. And so, everybody who has a good idea should somehow bring the idea to DARPA.

I do not know if that is the answer, but it does seem to me that there ought to be a place. You recommend an acquisition guide.

I would like it to be—I know about the simple solution to the complex. But, nevertheless, it should be as simple as possible, that there is one place to go to get started and let somebody else do the navigating, rather than, in the case of a small company, a small business, a small college or university, it is very difficult to find the time and the resources to figure out how to navigate what is a minefield of bureaucratic traps.

Mr. SMITH. But if you could hit that one specific point. You have got a good idea out there. And I know this works, because we all have examples of companies we know that have technologies that have found their way into the field.

If you could hit on that one point, Mr. Kline. I mean, it is, okay, we have got some new way to defeat IEDs, some technology company out there, or some new, better material that is going to produce body armor.

What is the process? In an ideal world—well, forget the ideal world. How does it work right now? And how could it work better?

Mr. LEHMAN. Well, Joint Improvised Explosive Device Defeat Organization (JIEDDO) itself is sort of overwhelmed. JIEDDO itself is overwhelmed with too many ideas right now, and sorting through that process has been very difficult. Now, that is a schedule problem, and everybody wants to help with a very, very difficult problem.

But they have gotten thousands of ideas. And sorting through those ideas has proved very, very challenging for them. It is a staffing problem.

If we talk about the process in a sort of more regular basis, I suggest that maybe the DOD should reach out to the technology transfer offices in the colleges and universities and say, here are the kinds of things that we are looking for and provide them a list, so that they are not just looking for commercial applications for the technology, but they are looking for DOD applications for the inventions coming out of the universities and colleges.

Mr. SMITH. And how do those partnerships work? Because I know there is a ton of research going on in the university level.

And it is my impression, by the way—and we have had a lot of testimony about what does not work here. But by and large, we have generated a fair amount of technological solutions that have helped both in the military context and in the commercial context, as well. So, there is a process out there.

How does the coordination work between the military and the various research universities that we have in this country? Fairly well is my impression. But how could it work better?

Mr. LEHMAN. Well, I would say that it does work well at the research level and producing results.

I do not think there is a close enough tie between the research investment and the programs that could use it. And that could be fixed by some greater planning, you know, the research community that is making the investment in the university, working with the programs of record at that point and say, three years from now we should have some results here.

Where are you going to be in your program, and how will you be able to receive it? And that the money is POM'ed and planned at that point to start inserting the technology.

Mr. SMITH. I had one question, and then I will open it up to other members.

We have got a bill on the floor this week, as a matter of fact, dealing with the issues that we are talking about to some degree, which has to do with conflicts of interest between the public sector and the private sector, and focusing on—I think it might be more broad than just the military—but trying to place greater restrictions on the so-called revolving door of people moving from defense contractor companies into the Pentagon and the government and elsewhere.

I do not know if any of you are familiar with that. You are not. Okay. Well, all right.

The question I have is, do you have any specific guidance in terms of within that bill, because we are trying right now, and we have been successful to get some of the stuff out of there that could harm specifically DARPA.

And we mentioned—I think, Mr. Lewis, you mentioned you have the mid-career researchers at DARPA who we bring in there, because they have specific experience in the private sector with a given technology. They work on it and then go back out.

That has not being prohibited, but there are some restrictions on working on a project within DARPA, specific to a given company, then going out and working for that company in less than a year.

Any thoughts on that?

Mr. LEWIS. You know, it is a rule that you see across the Federal Government and when—the rule being that if you are at least a senior manager, that you are not supposed to go back and lobby your organization or get contracts for your organization or do work for the organization for a year.

In general, I think people accept that. I think that people are comfortable with it.

You need to be careful that it does not close off some area of research. And that is where science is a little bit different from, say, contracting.

But my own sense is, the places where people have not observed this rule—and you may have seen the articles recently about the Department of Homeland Security having to adjust its regulations to make it clear that senior managers could not come back and lobby or search for contracts in less than a year.

Where they have not followed that rule, there have been problems. So, if there is a way to do that without hurting research, it sounds like a good idea.

Mr. SMITH. And it is possible. I mean, it is not—because we are getting concerns about, you know, it will limit DARPA's ability to get the best and the brightest. And I suppose the devil is in the details there, but I appreciate that perspective.

Anybody else?

Mr. THORNBERRY. Let me just ask. We have touched on it, but my question is, when you consider national security, what areas should we spend more research S&T money on?

I think you have said, and maybe you all agree, basic materials research. But I guess I am just curious, if you are going to place greater emphasis with where you spend your dollars on things that are the most important for national security, what are those areas?

Mr. LEHMAN. I would venture that cyber security is at the top of the list today. And we are creating a command and control system that is dependent on information. The net-centric, it is indeed the right thing to do to create a very effective command and control and lethal force.

But we are not paying sufficient attention to the security of the network and survivability of that network, because we are becoming more and more dependent on that information to conduct operations.

Dr. STARR. I would like to second that point. That was the thing I would emphasize most strongly. It is the type of things that we are seeing at DARPA right now, where they are re-changing the priorities for the Internet. Rather than connectivity being most important, it is information assurance.

And again, we have people in the audience here who are really expert in that.

And there is a second dimension also. And it is that the military is inherently mobile. And the way our infrastructure is designed, it is more for a static kind of situation.

And so, in reconceiving the network, it is how one would have many mobile users who have secure access and would be continually plugged in and available to deal with it.

So, I think those are the two most important issues that we could deal with.

Mr. LEWIS. I would kind of like to disagree a little bit. I used to have a bumper sticker, Mr. Chairman and Mr. Thornberry, that said "the country with the most physicists wins."

And I do think that physics is an area that we need to spend more on—chemistry, materials. We do a good job on nanotechnology, but there are other material areas that we do not do as well—direct contributions to the military.

Engineering—someone mentioned the large-scale integration problem. And that is an area of American strength, but it is an area where we could benefit from more research.

I agree that IT, computing sciences, broader than simple cyber security, is an important area. People say it is underfunded. It looks like there is a little bit of truth to that.

And finally, aerospace. So much of our money has gone to programs, that you see problems in things like keeping the wind tunnels open to do aerospace research.

So, those would be the five areas, I would think: aerospace, IT, engineering, chemistry and physics.

I am not a physicist, by the way.

Mr. LEHMAN. If I might add, I have here the Defense Science Board summer study from 2006, "21st Century Strategic Technology Vectors," which has done a very good job of laying out three or four vectors for technology research.

Mr. SMITH. A final question I had was, going back all the way to the beginning, we were talking a little bit—I think it was Lehman—you were actually talking about connecting the warrior to the technologist.

Now, we have jurisdiction in this committee over special ops, and have visited a lot of them. And it seems to be working fairly well in that area. They seem to be able to go directly to the people and say, this is the kind of gun we want, this is the kind of Intelligence, Surveillance, Reconnaissance (ISR) capability we want.

I can see that that would be unique to the special forces. Is that a larger problem for the rest of the military? And what would be an idea of how you would want to better connect the warrior with the people making the stuff that he needs?

Mr. LEHMAN. I would agree that special forces does that better than anyone else. And I think it is because of their size and their Title 10 authority.

The notion that I have in working in command and control is that we need to put these systems together, in peacetime or in garrison, with a cadre of operators and the contractors that are building these systems.

And we need to run these systems in peacetime, not in a scripted exercise where it is sort of scripted for success, but as a real experiment with simulation, and see what works and what does not work, as opposed to only putting this together in the field.

The intelligence community, since they are really working 24 hours a day, 7 days a week on intelligence problems, many of these systems come together that way in the intelligence community. They are real analysts working with technologists on day-to-day problems.

And the problem in command and control is that it only comes together in these scripted exercises or when we go to war.

Mr. SMITH. Well, let me just say, if could interrupt, because I think that is what is happening. In talking with people, prior to 2004 we had major problems in this area. In the last three years what I hear is we are doing better. And the reason is, we do not need the scripted exercises. It is happening out there in the real world, which is, of course, not the ideal place to learn——

Mr. LEHMAN. Right.

Mr. SMITH [continuing]. What equipment you need.

Mr. LEHMAN. And we have been evolving those systems in the field very rapidly with the contractors out there to great effect.

What is missing is the sustainment, because we will lose that capability, that software that has been written, because the training manuals were not written along with the software as it was built.

And so, that kind of capability will be lost, and we will have to rebuild it for the next one.

Mr. SMITH. We have to run across the street and vote.

Does anybody have anything else? I do not want to cut off—and get to the order here.

If not, we will probably submit more questions for the record to you, the ones we have in the book. And look forward to your responses and look forward to working with you on these problems.

This is very, very helpful. I thank all of you for your testimony.

And thank you, Mr. Thornberry and the members of the committee.

And with that, we are adjourned.

[Whereupon, at 4:36 p.m., the subcommittee was adjourned.]

APPENDIX

MARCH 14, 2007

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 14, 2007

The Testimony of
David H. Lehman
Senior Vice President and General Manager, The MITRE Corporation

BEFORE THE HOUSE ARMED SERVICE COMMITTEE, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES, ON HARNESSING TECHNOLOGICAL INNOVATION: CHALLENGES AND OPPORTUNITIES

Mr. Chairman, Honorable Members, thank you for the opportunity to appear before your Committee. My name is David Lehman and I am a Senior Vice President at the MITRE Corporation. I am also the General Manager of MITRE's Command and Control Center, which is part of the Defense Department's (DoD's) Command, Control, Communications, and Intelligence (C3I) Federally Funded Research and Development Center (FFRDC). Also pertinent to this discussion, I was MITRE's Chief Technology Officer for nine years, managing our internal research program. I would ask that my prepared statement be included in the record.

Steve Jobs of Apple said, "An innovation is an idea that ships." The idea may start as a technical curiosity, a result of scientific research. If someone can connect that curiosity to a solution to a real-world problem, an invention is created. If people or organizations adopt that invention, an innovation is created. Too often the research community lacks an understanding of real-world problems and the potential users do not know that the enabling technology exists. The result is too few inventions and even less innovation. To combat this, we must create an environment and processes that carry research results through invention to widespread adoption and, thus, innovation.

In my testimony today I will present four recommendations to improve both the processes and the environment in order to increase the yield of innovation from our science and technology (S&T) community. I will focus less on research—the creation of technical ideas, which might come from government laboratories, academia, industry, or amateur scientists—than on the management processes necessary to increase invention and innovation. These recommendations are:
1) Improve the alignment of S&T investment with warrior needs;
2) Improve the funding mechanisms to carry research results and inventions through to innovations;
3) Adopt open systems architectures for programs of record so that these programs can more easily accept and adapt to innovations; and
4) Change the business model used in programs of record to increase incentives for contractors both to meet requirements and to apply creativity in doing so.

The key to a good research program is to align investments with the goals of the organization or the needs of the end user. When an organization fails to achieve such alignment, the researchers tell the developers, "You don't use anything we invent" and the developers retort, "You don't produce anything we can use." This stand-off occurs because the two departments have not worked closely together to understand:

- The needs of the customer or the organization,
- The research problems,
- The research risks, and
- The funding profile that links the research schedule and budget to the production schedule and budget.

When an organization can solve these problems, it can put a plan in place that includes continuous dialogue around the inherent uncertainties in the plan, and adjust the plan as necessary over time. Optimally, this process enables the organization to bridge the chasm between research and production.[1] I should caution that if the linkage among the customer, the researcher, and the developer is too tight, the organization might fail to discover new approaches because the incremental improvements desired by the customer blind the developer to new, disruptive technologies[2] that offer vastly more efficient ways of solving problems;[3] consider the old observation that Henry Ford would have made faster horses if he had listened to his customers.

Government organizations have proven that they can achieve optimal alignment between research and development. The National Reconnaissance Office (NRO) of the 1970s and early 1980s offers an excellent example. The organization tightly linked its research investments in increased sensor sensitivity and satellite technology to production projects, resulting in continuous improvement in intelligence collection capability. The NRO could achieve this alignment of budgets and schedules partly because of its organizational structure, in which the users, the programs of record, and the research organization all reported to the same manager, creating unanimity of purpose and control. The NRO also had exceptionally strong and technically competent program offices—essentially technical peers of their contractors.

Beyond lack of better organizational structure and technically strong program offices, there are four additional reasons why most organizations do not achieve this alignment:

First, neither the research community nor the acquisition community fully understands the needs of the end user (in the case of the DoD, the warrior). A well-intentioned but overly bureaucratic documentation and review process hinders efficiency in requirements generation by unintentionally isolating the warriors from those who will design and build the system. The acquisition process believes that the specification is in essence flawless when the program begins and limits the interaction between researchers and warriors that would lead to acceptable—and feasible—tradeoffs in system design and functionality.

[1] For a good discussion of this topic, see Philip A. Roussel, Kamal N. Saad, and Tamara J. Erickson, *Third Generation R&D: Managing the Link to Corporate Strategy* (Boston, MA: Harvard Business School Press, 1991).

[2] See Clayton M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Businesses to Fail* (Boston, MA: Harvard Business School Press, 1997).

[3] William L. Miller and Langdon Morris, *Fourth Generation R&D: Managing Knowledge, Technology, and Innovation* (New York: John Wiley & Sons, 1999).

The formal research and acquisition process as practiced offers far too few opportunities for rich dialogue between the engineers, who know what technology can do but do not understand the real-world problems, and the warriors, who have the real-world experience but not the technological insight. 3M Corporation attributes its early success as a company on its strategy of placing its researchers in automotive production plants to understand the automobile industry's particular requirements for abrasives.[4] It is this dialogue, where the technical curiosity or idea becomes linked to the real-world problem in a give-and-take discussion, that leads to problem discovery, invention, and innovation. Today in Iraq we see rapid innovation with systems such as Command Post of the Future, FusionNet, and Cursor on Target because the technologists are in the field with the users, listening to their needs and rapidly adapting the systems.

To achieve this kind of interaction in the research and development cycle we need to create a development environment in which the warriors and the technologists interact continuously, experimenting with new inventions and applications, and rapidly incorporating those that prove themselves into the programs of record. As noted, some of this is happening in Iraq today, but many of the improvements will be lost because training and sustainment—which the acquisition process properly enforces for programs of record, though at the cost of acquisition speed—are often overlooked when quick-reaction capabilities are developed in the field. Particularly for programs that have a large information technology component, we must create a development environment in which the S&T community and contractors constantly test possible improvements by installing innovations and allowing cadres of warriors to interact with the innovative systems, understand the systems' utility, and provide feedback so that the developers can incorporate improvements into the systems. This represents a feasible but radically different development environment than the one that exists today.[5]

Second, the S&T community's research portfolio is not as well aligned as it needs to be to both the needs of the warriors and the programs of record that exist to satisfy those needs. Tighter alignment must come from joint management of the investments through continuous dialogue among warriors, researchers, and developers; otherwise, we will continue the pattern of research results that are never used and programs that are less technically advanced than they could be. Please note: only *part* of the S&T budget should be tied to user needs and existing programs of record. The S&T budget represents a portfolio of programs, some of which should support basic research, risky investments, and searches for disruptive advances to give our warriors a technological edge for which no program of record exists. Such disruptive technologies can have the highest impact, but they too will become innovations only if the system developers who understand the technology engage in a rich dialogue with the warriors to understand their problems.

[4] Jim Collins and Jerry I. Porras, *Built to Last: Successful Habits of Visionary Companies* (New York: Harper Business Essentials, 1997).

[5] For a more complete discussion of this idea see Victor A. DeMarines, with David Lehman and John Quilty, "Exploiting the Internet Revolution," in Ashton Carter and John P. White, eds., *Keeping the Edge, Managing Defense for the Future* (Cambridge, MA: Harvard University, The Preventive Defense Project, 2000), http://bcsia.ksg.harvard.edu/publication.cfm?program=CORE&ctype=book&item_id=143

Third, research schedules are not aligned with acquisition schedules. Achieving such alignment is understandably difficult, because research does not follow a timetable. Scientists cannot invent on the government's schedule. Government programs must learn to manage the inevitable uncertainty. Service laboratories regularly present inventions to acquisition programs, but the acquisition program usually has little latitude to make changes: the program has a contract and a contractor, a budget, a schedule, and a system design. Inserting the invention, while it might benefit the warrior, would represent an unplanned expense and a schedule slip. Acquisition programs must plan better so that they have the flexibility to accept promising inventions. This can occur only if the acquisition process accommodates advanced collaborative planning by the program and research communities and features constant communication throughout the research and development cycle to manage the uncertainty.

The fourth failure in alignment relates to funding. The research and acquisition communities must plan for success from the moment they embark on a research project. The funding profile in the Program Objective Memorandum (POM) must bridge from research funding through acquisition funding. Too often research programs, Advanced Concept Technology Demonstrations, Joint Expeditionary Force Experiments, and the like validate operational needs, but the budget lacks funding for follow-on development, acquisition, and fielding. It is also axiomatic in all research that some programs and experiments will fail to achieve their intended results, which creates uncertainty in the budget.

To deal with this uncertainty the acquisition community needs to have a set of funds available that allow it to harvest the best ideas that have achieved practicable results. In economics, this approach is called "real options." Having many investments in a portfolio creates options for the investor. Some of them do not succeed, but others do, and the investor can choose to adjust the budget and allocate more funding to those that have proven their worth. Having a line in the POM that gives program managers the flexibility to apply funds to research investments as they mature and carry them into programs of record will increase the innovation yield from the S&T community. This line item should be large enough to harvest some, but not all, successes, forcing the services and programs to prioritize user needs and control budgets.

As a corollary to this observation, we must improve our ability to manage failure. If we recognize and deal with failure early, we can afford more new starts.

The same funding gap characterizes other innovation programs run by the DoD. The Small Business Innovation Research (SBIR) program offers an effective mechanism for funding small innovative companies, but many promising ideas are never harvested for lack of the funding needed to bring the ideas to development and lack of connections among the company, the programs (and their prime contractors), and the warriors who could use the invention. The following quotation comes from Helen Greiner, co-founder and chairman of iRobot, a company that develops robots for the DoD and commercial markets:

> Risk and Reward – There were numerous times when we "bet the company." Like most innovative companies, we shouldered high risk ventures. We were rewarded for our successes; but, there is a problem with how the government deals with new technologies. The government doesn't balance higher risk with higher reward; and, in fact, seems to negotiate lower profit with small companies. Perhaps this is because of the lack of understanding small companies possess regarding how to "play the game" vis-à-vis larger defense companies. The transition from prototype to production is a critical step for innovative companies. The government's support for developing technology (e.g., SBIRs) is not in harmony with the lack of support to transition that technology into production. I'm left to wonder how many great ideas die on the vine...

Once programs have achieved alignment in the four areas I have mentioned, they must ensure that the systems they field are designed with open architectures that have defined interfaces and use well-known and accessible commercial standards. A good architecture allows a system to be modified easily, and thus to accept with relative ease some—though not all—future innovations and improvements. Google, eBay, and Amazon do this very well. They have invested in an infrastructure that features well-defined interfaces and enables their own employees and their business partners to experiment and add innovations with great success.

The DoD acquisition community is striving to build systems with open architectures, but to meet this goal the DoD must find a new business model for its contractors. Under the standard model, the DoD lets a contract for an entire system, usually for its entire lifecycle, which gives the contractor little incentive to design an open system. On the contrary: such a model motivates contractors to design proprietary systems, tying future profits to their exclusive knowledge of the system. To avoid this outcome, the DoD should let a contract for a base infrastructure with as open a design as possible. It should then let separate, smaller contracts for the applications that will ride on the infrastructure and bar the infrastructure contractor from bidding on these applications. Many smaller contracts versus a few larger contracts present a radically different model for the contractor community and the DoD must construct the model so that contractors can profit from it—and will therefore dedicate their best efforts to achieving program objectives. The contracting community will undoubtedly find it difficult to adapt to this change. However, such a structure will allow the DoD to become a faster adopter—and beneficiary—of innovations.

In summary, to increase the yield from our S&T investments I recommend that the DoD strongly encourage the S&T community, the acquisition community, and the warriors to manage the acquisition process *as a team*. Technologists and program offices should together engage in dialogue with the warriors about needs and technical solutions. They should agree on investments in promising technologies. The services should craft the POM for success in the resulting investments using a funding line that allows them to harvest successes. Together they should continually review progress and adjust schedules to align maturing solutions with the POM money and programs of record. To the extent possible, programs of record should feature architectures that allow easy adaptation to new innovations. Finally, acquisition strategies should incorporate incentives for open architectures, competition, and innovation. I wish to point out that the DoD already possesses the authority to act upon all of these recommendations with the exception for some of the flexibility in the POM line.

Finally, I would like to mention the possible contributions of FFRDCs in the context of these recommendations. FFRDCs could play key roles because of their combination of technical expertise and their inherent, government-mandated impartiality. This impartiality is especially important, because commercial organizations can freely share their latest findings with FFRDC staff and because FFRDCs have no commitment to a particular vendor or system.

The strong technical talent of the FFRDCs can augment the expertise of government program offices, enabling them to interact with their contractors from a position of peer-level understanding of technology. This would allow the program managers to use technical, measurable criteria to determine which innovations actually perform best.

To assist in increasing the yield of innovations from the wealth of technology available, FFRDCs could work with the S&T and acquisition programs to accelerate technology transitions from the government S&T community, industry, and academia. Their access to both government information and commercial proprietary information would permit FFRDCs to conduct impartial evaluations of inventions stemming from a broad range of the research community and to select those most relevant to identified needs and most likely to succeed in fielded programs.

I believe that implementing the recommendations outlined above will keep the United States at the forefront of applied technological innovation, and contribute to the success, and the safety, of our warriors.

Thank you, Mr. Chairman. I would be happy to answer questions.

Testimony
House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities
"Harnessing Technological Information: Challenges and Opportunities"
March 14, 2007
James A. Lewis
Center for Strategic and International Studies

Let me being by thanking the committee for this opportunity to testify before it on this important subject. I am going to make four points in my testimony that I will summarize for you now. First, technological leadership has contributed to U.S military superiority and economic strength for more almost seventy years. It is crucial for U.S. economic and military strength. Second, globalization and other changes means that U.S. share of innovation will decline, as other nations increase their efforts in science and technology. Third, U.S. policies reinforce this decline. These policies include under investment in science, a more difficult regulatory climate, and the unintended effects of many of the policies put in place since September 11, particularly in regard to immigration and technology transfer. Fourth, while the U.S. faces challenges when it comes to technological leadership, some of its own making, it also has opportunities to respond in ways that will advance its security and economic interests.

The key to technological leadership is innovation. Continued technological leadership depends on the U.S. capacity to innovate. Innovation is the ability to use knowledge to create new or better goods and services. The U.S. innovation system, with its mix of university research, entrepreneurship and venture capital is crucial for a steady flow of ideas that benefits both the commercial market and a military that often relies on commercial technology. The U.S. has been one of the world leaders in innovation, and our political and social makeup may provide America with something of an advantage over other nations when it comes to the ability to innovate. The question is whether this comparative advantage is, by itself, enough in an era of heightened global competition.

The first thing to note, perhaps, is that there is a strange anomaly in these concerns over the potential loss of technological leadership. That anomaly is that the U.S. spends more than any other nation on science and on research and development. The U.S. spends more that the next five nations combined. It is reasonable to ask how there can be a problem when we are spending so much more than other nations.

The answer is also relatively simple. We are not spending enough to maintain our lead, and we are not spending enough on the things needed for military technology. While our spending levels are flat, spending in other nations is increasing. If these trends continue without change, the long term result will be that the U.S. will no longer have the lead in important technologies.

The picture is complicated because, when it comes to research, nothing ever happens quickly. The results of misinvestment and underinvestment in science can take years to appear. We are coasting on the results of Federal spending from the 1960s and the 1980s, and the boost from that spending has not yet disappeared.

The picture is also complicated because the data is ambiguous. It is hard to measure innovation, so the normal practice is to use proxies, things that we know are part of innovation and science and which are easier to measure. Proxies for innovation include things like the numbers of patents awarded to a particular country, the number of Ph.Ds and engineers it graduates, or the number of scholarly articles published by its scientists. When we look at this data, it is not immediately clear that the U.S. is losing ground.

There are, however, some troubling trends. In a few key areas of research, scientists in other nations are publishing more than their American counterparts. The number of U.S. authored papers increasing by only 13% between 1988 and 2001 while the number of papers authored by Europeans increased by 60% (and Europe overtook the U.S.) while the number of papers authored by Asians more than doubled, increasing by 120%. Even more worrisome is that half of the U.S. publications were in the life sciences, whereas other nations were concentrated in the physical sciences. The age of our technological workforce in some key areas, like aerospace, is another troubling trend. Many scientists and engineers will retire in the next few years and will not be replaced. From an economic standpoint, this may not be bad – we do not want to train engineers only to find that there is no work for them – but from a national security perspective these are warning signs that suggest that the U.S. may want to consider whether if it is paying enough attention to the connection between science, technology and security.

Answering this question requires a look at the larger international environment. We are in a very different international environment. In political, economic and security terms, this environment is changing rapidly and in ways that we did not expect when the Cold War ended that challenge U.S. leadership and security.

Part of this challenge is the result of what we call globalization - the increasing integration of national economies into a single market. Globalization tends to diffuse technology around the world. Globalization has eroded the national character of science, as research is increasingly carried out by multinational teams, but it has not changed the need for nations to draw upon science for their security. Part of the challenge also comes from the rise of strategic competitors, national like China or India, and perhaps Brazil or even Europe in the distant future. These strategic challengers have seen how important science has been to U.S. military leadership and they seek to copy what we have done.

Saying that globalization creates security challenges can easily lead to the wrong conclusion. Some might argue that if we could slow or restrict globalization, the U.S, would be more secure. Unfortunately, this is completely wrong. First, globalization is the U.S.'s idea. It is the result of long standing foreign policies as to how the world should work – that a world based on free trade, rule of law and democratic government would ultimately be safer and more prosperous. Second, the U.S. has benefited as much or more from globalization as has any other nation. Finally, reversing globalization is out of the question unless we are willing to accept wrenching dislocations and a loss of wealth and power for the United States. The real question is how do we take advantage of the opportunities globalization creates while minimizing the risks that come with these opportunities.

Globalization is an opportunity and a challenge. A related opportunity and challenge comes from Asia's economic ascent. The nations that lie along the Pacific Rim are now the central focus of global economic activity. The U.S. is part of this, but the most dynamic growth has been in Asia, first with Japan, then with Korea and Taiwan, and now with China. Asian nations now hope to repeat their success in manufacturing in scientific research. If Asia is today the world's factory, its nations hope that tomorrow it will also be the world's laboratory.

Part of the challenge also comes from changes in the ways societies create wealth. The most important of these changes is the transition to an information economy. An easy way to understand this transition is to look at earlier examples. In the 1800s, we saw a transition from agriculture to industry and manufacturing. This transition meant that the best way to generate wealth lay in industry, not farming. Now we are seeing an economic transition from manufacturing to information. This means that the best way to generate wealth will be in the creation of new knowledge, not in industrial production. However, while this transition away from manufacturing may be good for the U.S. our economy, it does have implications for U.S. leadership in military technology.

The cumulative effect of these changes is to put U.S technological leadership under some pressure. Combined with problematic U.S. policies, they create a new kind of risk for national security. The best way to describe this risk is that the vigorous research and technological base that has given the U.S. a military advantage for decades is in danger of being eroded.

The U.S. and other nations realized in World War II that sustained scientific research provided military advantage. The United States created institutions in the 1940s and 1950s to support scientific research for national security, including DARPA, the service labs, the National Science Foundation and others. These Federal institutions build upon and are closely intertwined with America's strong University system, and the graduate research programs found at these universities. The U.S. system of innovation, with its mix of university and federal research, entrepreneurship and venture capital, provides a steady flow of ideas that benefits both the commercial market and a military and it is the envy of the world.

Two sets of problems put U.S. innovation at risk. Congress can play a central role in addressing both sets of problems. The first set of problems has to do with funding. The second set of problems has to do with regulation. Erosion of capabilities should come as no surprise that if the trends are to under-fund and over-regulate.

Funding for research is the most important of these problems. While the U.S. continues to lead in many research areas, its investments are not enough to sustain this lead over the next decade. The problem lies with the absolute levels of investment, the distribution of investment among research activities, and the rate of change relative to other nations. U.S. spending in scientific research areas that are key to national security is flat or declining while other nations are accelerating their spending. This is not a long-term strategy that is likely to produce success.

Federal funding for basic research in engineering and physical sciences has experienced little or no growth in the last thirty years. As a percentage of GDP, funding for physical science research has been in a thirty-year decline and has fallen by about half. Total federal funding for R&D

was essentially flat from 1988 to 2001. Spending on mathematics research was roughly $190 million in 1985 and $200 million in 2004; spending on physics was flat between 1985 and 2001 and there were only slight increases in funding for chemistry. Funding for engineering research increased from approximately $6 billion to $9 billion between 1988 and 2001, but funding for some key research areas, such as electrical engineering, remained essentially flat.

The effect on security of underinvestment is acute and damaging in specific research areas. These include physics, aeronautics, mathematics, computer sciences, and engineering. There are three reasons for emphasizing the dangers of underinvesting in these areas. First, research in these areas provides the basis for improved military performance. Second, in relative terms, these areas have been the most seriously underfunded. Third, advances in these research areas enable other areas of scientific research – by providing better sensors and measuring tools or improved computing power.

The problem of underfunding is compounded by changes in research and development in the Department of Defense and in the private sector. In the past, about three percent of DOD spending on procurement ultimately went to R&D. However, the decline in procurement of new equipment has reduced the amount of funds for technological innovation for the military. In addition, government and private defense R&D investments are skewed - understandably - toward near-term priorities (e.g., upgrades or replacements for existing systems) rather than fundamentally new capabilities. Additionally, some research problems are too expensive for any company to undertake. The combination of changing research priorities in DOD and the private sector means that some key research areas are not adequately funded.

Another set of U.S. policies also threatens technological leadership. These are changes in immigration policy. It is useful to remember that U.S. national security and military power was strengthened in the 20th century by an influx of foreign scientists fleeing unstable conditions in Europe. The universities and institutions that received these scientists became global leaders in research, a role which they continue to play. Having these leading universities benefits the U.S., as leading students from other nations come to the U.S. to study and contribute to research.

However, several factors have made the U.S. a less attractive destination for scientific talent than it once was. Measures imposed in the attacks of September 11 have the unintended consequence of deterring some researchers from coming to the U.S. Other changes prevent researchers form staying here once they complete their educations. This is particularly damaging - when a foreign student has completed their training and is ready to begin work, U.S. policy is to have them leave and work in another country. At the same time, other nations have recognized the economic and military advantages provided by scientific leadership and have attempted, with some success, to capture a greater share of scientific talent and to duplicate the success of research centers found in the U.S. This means that the U.S. faces new competition for scientific talent at the same moment that it policy is to discourage needs to compensate as foreign supplies of scientists and engineers shrink in the face of increased demand from other countries.

U.S. restrictions on technology transfer also works against maintaining technological leadership. In some areas, there are restrictions that prevent scientists from exchanging unclassified information or working together on research projects. In other areas, restrictions on U.S. exports have encouraged other nations to invest in their own research and technologies. The unintended effect of these restrictions, and the restrictions on immigration, has been to create incentives for people to move research outside of the United States. The unintentional effect of some U.S. policies is to create new competitors.

It is worth noting that there is something of a tendency to overemphasize the negative in this debate - whether it is hand-wringing about manufacturing or the constant barrage of news and reports about the weaknesses of American elementary and secondary education. A few historical anecdotes help to illustrate this. In 1957, after the Soviet Union shocked the U.S. by launching the first satellite, President Eisenhower's science advisor predicted that because of the Soviet lead n math and science education, they would surpass the U.S. in ten years. He was wrong. In the 1980s, many pundits said that Japan's rapid growth, astute trade policies and dominance of manufacturing would make them the leading economic power within a few years. They were wrong as well.

Now we hear similar predictions about China and other nations. In thinking about these latest predictions, it is useful to ask why the Soviets or the Japanese did not succeed in displacing the U.S. Some of the reasons for this have to do with the weaknesses found in those countries. Every nation has strengths and weaknesses, and we want to be careful not to exaggerate or misinterpret. The U.S. has some unique advantages that other nations cannot match. China, India, Europe and the other competitors the U.S. faces today all have their own problems and handicaps.

A more important factor, however, in explaining why these predictions were wrong, is the U.S. response. In each case, the U.S. changed is policies and practices to respond better to foreign challenges to its technological leadership. In the late 1950s, government policy was most important and the U.S. responded with new programs to expand scientific and mathematical education. In the late 1980s, the private sector response was important as U.S. companies changed how they operated to become more competitive. The U.S. has had an advantage in its ability to blend public and private sector that other countries sometimes find hard to match. The lesson from this is that if the U.S. can find the right set of responses, the problems it faces today are eminently manageable.

There has already been some progress in the search for the responses needed for the new international environment. A number of eminent studies and commissions have reported and made their recommendations. The President announced the "American Competitiveness Initiative in his 2006 State of the Union Address. And both parties in Congress have put forward programs for strengthening innovation.

However, these are only initial steps. Both the government and the private sector still have much work to do. As the Committee contemplates next steps on the challenges and opportunities the U.S. faces in harnessing technology for national security, it may wish to consider these general recommendations.

First, make the promotion of innovation a benchmark and a goal for policy and law. This may require that the U.S. streamline and simplify the regulatory burden for innovation. The U.S.

tends not to ask whether a proposed action will accelerate or degrade its innovative capabilities. In the past, it could afford this but that may no longer be the case.

Second, the U.S. should look identify where government action is appropriate and can be effective. One area is in the funding for basic research in the physical sciences. Absent government support, the U.S. lead in these sciences will continue to decline.

Third, look for ways to expand and exploit our comparative advantage. Our market-oriented economy gives us an advantage over many countries, and policies that enable markets will help innovation. Measures that strengthen the institutions we have created to link science, technology and national security will provide immediate benefits. These institutions include – DARPA, the service labs, NSF and NIH, and of course the graduate research programs at our Universities and keeping them strong is crucial to American power.

Fourth, the U.S. would gain from initiatives that embrace international cooperation. The U.S has benefited greatly from globalization and efforts to restrict globalization will backfire. In defense, closer cooperation with allies in research, development and production can provide real advantages to national security.

All of these recommendations may sound very far from the Defense policy. They certainly are not conventional national security issues. The challenges the U.S. faces today are also not conventional. In this changing security environment, an accelerated ability to create new technologies will remain crucial to America's security.

I again thank the Committee for the opportunity to testify.

Statement of Dr. Brian S. Cohen
Institute for Defense Analyses
Assistant Director, Information Technology and Systems Division
On
Integrated Circuits Supply Chain Issues in a Global Commercial Market – Defense Security and Access Concerns
Before the
House Armed Services Subcommittee
Terrorism, Unconventional Threats and Capabilities

March 14, 2007

Mr. Chairman and distinguished members of the Subcommittee, I am pleased to speak to you today about efforts to mitigate potential national security concerns resulting from the off-shore migration to major elements of the Integrated Circuit (IC) industry. I have spent much of my career at the Institute for Defense Analyses (IDA) working to help Department of Defense (DOD) understand and assess the emergence of what is now clearly a global IC market dominated by commercial interests and supplied by what is frequently a non-U.S. industry base. In 2002, I started work on DOD efforts to deal with concerns about the declining domestic sources of ICs and consequent increased dependence on foreign sources for critical ICs. Much of this work focused on the Trusted Foundry Program and the accreditation of Trusted Suppliers, particularly for custom-designed ICs[1]. While more work is required to find solutions for all types of ICs and for the broader elements in the supply chain, the Department has had considerable success in using the Trusted Foundry and Accredited Trusted Suppliers for custom-designed ICs. My statement today addresses this work.

Background

The information revolution in the recent past has had a profound effect on DOD. Looking back over the last fifty years, there are two clear technical pillars for the information revolution, microelectronics, as exemplified by ICs, and information technology (IT). The synergistic emergence of these areas has fueled dramatic innovation. DOD had an important and leading role in the development of the technologies and industrial base for both microelectronics and IT and without them key DOD strategies such as network-centric warfare would not be possible. Nevertheless, here we are today, struggling with change in both of these areas. A few decades ago both the microelectronic IC and IT industries had major market segments in Defense, but both have become primarily commercial. These days the DOD market, even taken in its entirety, is today a small customer for the IC industry.[2] Defense performance and operating

[1] Also called Application Specific Integrated Circuits (ASICs).

[2] A general rule of thumb is that a fabrication plant requires 3X its capitalization in annual revenue to make business sense. For a $5 billion plant this is $15 billion in annual revenue. IDA estimates that DOD (through its suppliers) purchases about $1 billion annually in military/aerospace ICs, and perhaps $2-4 billion annually of additional commercial ICs. While a detailed census is difficult to obtain, there seems to be no business case for a captive defense state-of-the-art fabrication.

environment requirements can differ from commercial needs and are often sensitive from a security perspective. Captive DOD IC capabilities are very expensive and difficult to keep at the leading edge, so DOD struggles with how their specialized needs can be met by commercial-focused sources. A recent Defense Science Board[3] examined these issues and some recommended actions. The report, while recognizing that the domestic IC industry was being driven offshore primarily by commercial factors, suggested that a long-term solution would be to establish domestic IC competitiveness as a national priority.

What are the Defense Security and Access Concerns?

ICs are extensively used in DOD computing, communications, and sensors. Most of these ICs are catalog, off-the-shelf items, such as processors and memories. However, some IC applications require specialized functions and/or have unique military performance demands. Such ICs are custom-designed and manufactured. Custom-designed ICs are generally the most security and access sensitive ICs in defense systems, as they may contain key intellectual property (such as algorithms) and because their proper functioning may be the crucial element in system performance. These custom-designed ICs are also more easily targeted by adversaries as they are tested by a relatively small user base for use in a limited number of applications. On the other hand, for memory ICs that are widely used by millions in the civilian sector, successful targeting and modification of such a commodity product is more difficult.

The primary national security concerns related to ICs are:

- Theft of important intellectual property such as algorithms encoded as part of the chip design
- Tampering with IC function thereby potentially causing defense systems to be ineffective, unavailable, or to allow unauthorized access
- Denial of access to advanced technologies and supplies, resulting in only older ICs being available for defense use

One might ask whether it is actually feasible that an adversary might steal intellectual property or tamper with defense supplies. To perform these nefarious acts, an adversary (whether nation state or individual actor) needs to:

- Perceive some benefit from the exploitation (motivation)
- Have the capability to perform the exploitation (capability)
- Have the opportunity to perform the exploitation (vulnerability)
- Have confidence of success (ability to target/avoid detection)

Although I cannot describe the details of the threats, vulnerabilities and capabilities in this forum, IDA studies and analyses have identified plausible instances where these threats to IC integrity are real.

One way of understanding an area like tampering is to look at counterfeiting which is a subset of tampering. The motivation for counterfeiting is usually monetary and the rate at which this

[3] *Defense Science Board Task Force On High Performance Microchip Supply,* February 2005, http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.

problem is found in industry indicates that this is more than sufficient motivation.[4,5] Detected counterfeit ICs are usually found because they malfunction or are substandard,[6] but a good counterfeit or tampered IC may appear by any measure to be a good part. These seemingly good but counterfeit parts are not likely to be detected. The alarming thing about counterfeiting is that we assume that the motivation for the observed counterfeit is monetary, but that may not always be the case. The mere fact that counterfeit ICs have entered the defense supply chain and have been found (because of their failure), demonstrates the feasibility of a tampered part with malicious intent also being inserted into the supply chain.

Finally, it is important to highlight that custom-designed and custom-manufactured ICs constitute only a small portion of Defense IC purchases. Most ICs used in DOD systems are catalog items that are mass-produced and, although they are not as easily targeted, there are security and access concerns with these products. It is also important to note that while ICs are but one element of the supply chain, there are serious concerns about the loss of domestic capability in other areas of the supply chain. IC packaging and assembly have already moved off-shore, and it makes little sense to go to great lengths to obtain trusted ICs only to ship them to some foreign company for packaging and assembly. A recent report by the National Research Council highlighted concerns about the printed circuit board industry moving offshore[7]. The Department will need to consider security and access concerns for the entire supply chain.

Trusted Foundry and Accredited Trusted IC Suppliers

The Trusted Foundry Program, initiated in FY 2004, leverages a contract with IBM to aggregate purchases of leading edge (CMOS/SiGe 90nm – 130 nm currently) IC manufacturing technologies for use in defense applications. As required by contract, the contractor upgraded their facilities and implemented enhanced security procedures, creating the Department's first Accredited Trusted IC Supplier. The Office of the Secretary of Defense (OSD) tasked the National Security Agency (NSA) to stand up a new office to manage this contract and, in response, NSA created the Trusted Access Program Office (TAPO) to perform this function. OSD also requested that NSA expand the ranks of suppliers capable of providing trusted ICs, and NSA implemented the trusted IC supplier accreditation. Just to summarize the difference between these two efforts:

- Trusted Foundry – Aggregated DOD buying (through TAPO) of ICs manufactured by the Trusted Foundry contractor as an Accredited Trusted IC Supplier. TAPO assists in the aggregation of defense purchases.

[4] *Counterfeit parts nettle buyers, China seemingly unable to stem tide of bad components*, Electronics Supply and Manufacturing, 08/18/2003 (http://www.my-esm.com/showArticle.jhtml?articleID=13100410).

[5] *Bogus! Electronic Manufacturing and Consumers Confront a Rising Tide of Counterfeit Electronics*, M. Pecht and S. Tiku, IEEE Sprectrum, May 2006.

[6] Panther Electronics of Fort Lauderdale, FL, was indicted by a federal grand jury on charges related to the sale of parts used in radar and communication systems on several military aircraft. Panther is accused of selling more than 400 microcircuits and connectors to the Air Force and Navy for use on F-14, F-15, and B-1 bombers. Random testing by the Defense Department found that approximately 20 percent of the parts purchased were either non-conforming or counterfeit. (source, Defense Supply Center Columbus, DLA/DSCC).

[7] *Linkages: Manufacturing Trends in Electronics Interconnection Technology, Committee on Manufacturing Trends in Printed Circuit Technology*, National Research Council (2005) (http://books.nap.edu/catalog.php?record_id=11515).

- Accredited Trusted IC Supplier – Supplier that is accredited as meeting the Trusted Supplier criteria. Customers go directly to the supplier

It is important to note that while the Trusted Foundry Program was created to manufacture ICs, reengineering the business structure to aggregate provided purchases across programs. This aggregation of purchases is an important parallel innovation, which has resulted in a substantial improvement in access to advanced technologies and cost savings. Multi-project wafers[8] and sharing both the access fees and infrastructure allowed customers to achieve substantial savings.

The Trusted Foundry Program is funded through equal investments from DOD[9] and NSA as well as from direct program reimbursements for acquisitions. The DOD share was approximately $31.2 million in FY 2005 and rises to $40 million in out years. The TAPO has made significant efforts to connect customers with the Trusted Foundry Program and in FY 2006, more than $100 million in business was performed through the program.

As a business approach, IDA views the Trusted Foundry to be successful. To date, 26 program requirements have been fulfilled. In FY 2006, 13 multi-project wafers were assembled and manufactured with an average of 15 IC designs on each. TAPO estimates in excess of $160 million in savings over comparable spot prices.

IDA's work on the Trusted Foundry

In 2002, during a cyclical downturn in the IC industry, it appeared that most, if not all, new state-of-the-art IC fabrication plants were being planned for construction off-shore. IDA was asked by OSD to assist in responding to Congressional concerns about whether a captive foundry could address security issues and retain domestic control of the capability. We found that a captive domestic capability would be far from economical and would be challenged to achieve and sustain leading edge technologies. Our research further concluded that while the current business structure was low cost, it did not support key military needs or address security requirements. The IDA study recommended a restructured approach that called for cooperation with commercial industry. At the same time, NSA, looking at how to meet its needs for specific ICs, had identified a potential approach using a take-or-pay arrangement with a commercial (domestic) IC firm (IBM). This became the basis of the Trusted Foundry Program.

In February 2003, IDA was asked to evaluate a technical proposal from NSA and IBM. IDA' assessment was positive, but recommended that the endeavor be Defense-wide, rather than focused solely on NSA. Subsequently, the Department moved forward with the Trusted Foundry as a DOD-wide effort. The Trusted Foundry Access program office (subsequently renamed to the Trusted Access Program Office (TAPO)) was established at NSA in January 2004, providing initial guidance and immediately kicking off an effort to bring in additional suppliers. The initial

[8] Multi-project wafers (MPWs) take several integrated circuit designs and combine them onto a single manufacturing run, thereby distributing the significant non-recurring expenses. These savings can be significant. It is important to note that the TAPO manages the aggregation of customers into MPWs, although contractors actually will perform the final merger of the designs into a single manufacturing run. At this time, TAPO only aggregates for production through the Trusted Foundry.

[9] The DOD funding is from PE 0605140D8Z (http://www.dtic.mil/descriptivesum/Y2007/OSD/0605140D8Z.pdf).

guidance, (which remains in effect today) required that programs with high mission assurance requirements manufacture custom-designed ICs through a "trusted foundry service."[10]

In order to leverage and be harmonious with other efforts, the concepts of how to specify trust for IC suppliers is based on the ideas already established in the information/mission assurance area. The DOD policy[11] requires that custom-design ICs for high Mission Assurance Category (MAC)[12] and confidential environments be obtained from an Accredited Trusted IC Supplier.

In early 2005, IDA assisted TAPO with a survey of industry interest in trusted supplier accreditation. There was strong interest from industry, and subsequent efforts have resulted in 6 companies becoming accredited (including 2 Rad Hard and 1 Compound Semiconductor) with 8 more accreditations in process.

Since then, IDA has helped OSD to clarify the concepts and required policies. A summary of the key policy concepts was presented at GOMACTech-2006.[13] The recent focus of work has been on extending the concepts to cover a range of assurance requirements[14] (e.g., moderate assurance levels as well as high) and to address defense requirements for all types of ICs beyond custom-designed.

While Accredited Trusted IC Suppliers provide one element of defense, IDA has continued to examine a range of approaches to addressing the security and access concerns. IDA has recommended that the Department also consider techniques such as anonymity in acquisition, encryption of designs and authentication.

DARPA was an early participant in the Trusted Foundry Program and was interested in identifying research opportunities that could address the concerns of IC security. In August 2005, IDA held a workshop at the request of a DARPA Program Manager with the objective of exploring research opportunities that hold promise for revolutionary advances in protecting the security and integrity of the microelectronic chips, primarily for defense or National Security applications. A small group of experts were invited and various techniques and technologies were discussed that might protect against the theft of intellectual property on the chip or unauthorized modification of ICs. A broad portfolio of techniques was considered for addressing these two concerns, including digital watermarking, steganography, self-test, verification, validation, hardware/software co-implementation, and secured programmable gate array devices. Some classified techniques were also discussed such as design obfuscation, anti-tamper techniques, secured PKI, and design encryption.

[10] Initially "trusted foundry service" implied that the ICs needed to be manufactured through the Trusted Foundry, but today, this is interpreted as being provided by an Accredited Trusted IC Supplier.

[11] Under Secretary of Defense (ATL)/Assistant Secretary of Defense (NII) Memorandum, *Interim Guidance on Trusted Suppliers for Application Specific Integrated Circuits (ASICs)*, January 27, 2004.

[12] DOD Directive 8500.1, "Information Assurance," October 24, 2002, (http://www.dtic.mil/whs/directives/corres/pdf/850001_102402/850001p.pdf).

[13] *Perspectives on Defense Trusted Integrated Circuit Policy*, paper presented at Government Microelectronic Applications & Critical Technology (GOMACTech) Conference - 2006, Unclassified, March 2006

[14] The initial policy required that only high mission assurance required the use of the Trusted Foundry. Extension of the policy to define how to handle more modest mission assurance requirements is more challenging.

The Trusted Foundry and Broader Concerns

DOD depends strongly on global commercial sources for the majority of its IC purchases and many of these are likely to continue to come from foreign sources. These ICs are not likely be supplanted by either the Trusted Foundry or by Accredited Trusted IC Suppliers. The Trusted Foundry/Supplier, in its current form, is oriented towards addressing immediate security and access concerns by partnering with domestic suppliers. It has been successful partly by enabling industry to reap the benefits of a differentiated "trust" market, and in some cases a managed customer base. While the criteria for a domestic supplier to become trusted (i.e., cleared facility and personnel) is reasonably achievable and affordable, large foreign based commercial firms will not be able to readily clear their facilities and personnel.

Additional DOD initiatives are likely to be needed to address the broader or long-term problems, including the issues surrounding mass-produced ICs. Another challenge is to how to obtain ICs from foreign sources and have some level of assurance despite their coming from foreign sources. For commodity ICs, the vulnerabilities and affordable mitigating techniques are markedly different from the techniques appropriate for custom ICs. There are alternative practices, such as anonymous acquisition of ICs, which can protect the identity of the customer (i.e., defense program offices) and provide a reasonably effective and affordable approach.

In the long-term, in order to fully leverage the global commercial market for ICs, DOD will have to come to terms with some key research challenges:

- How can DOD trust (at some level) foreign suppliers?
- How can DOD trust domestic suppliers (at some level) in the face of potential foreign influence or exposure to insider threat or criminal acts?
- How can DOD trust ICs (at some level) from suppliers who are unable or unwilling to become accredited?
- How can DOD still obtain ICs with specialized performance when commercial suppliers are not interested in the relatively small defense market?

The IC industry continues to consolidate driven by increasing fabrication plant costs, and by 2012, it is expected that number of state-of-the-art fabs will plummet.[15] It is entirely in the realm of possibilities that in the future, there will not be domestic fabs available and the Department will have no choice but to turn to off-shore sources for IC manufacturing. IDA believes that national security interests are best protected by maintaining a strong domestic IC technology and industrial base.

Summary

The information economy is built using semiconductors increasingly supplied by a fast growing, off-shore industrial base. The movement of the domestic industrial base off-shore has generated serious concerns about both security and access to advanced technology, especially for our information-dependent defense systems. Security concerns include both theft of intellectual property related to IC design, a special concern for custom-designed IC, and the potential for tampering with the semiconductors used in our defense systems. The DOD's Trusted Foundry

[15] *IC manufacturing set for restructuring*, EE Times, 11/07/2006.

Program and the complementary Trusted IC Supplier Accreditation were specifically designed and implemented to mitigate these concerns as quickly as possible. The Trusted Foundry Program aggregates defense IC purchases and has generated substantially better access to leading technologies at much lower cost. The Trusted Foundry/Supplier approach should continue to be effective for custom-designed ICs while there remains some domestic fabrication capability, however for broader types of ICs and for other elements of the supply chain, other approaches to addressing the security and access concerns will likely be needed. The Trusted Foundry and Accredited Trusted IC Suppliers have had notable success addressing the security and access issues related to custom-designed ICs.

Mr. Chairman and Members of the Subcommittee, I thank you again for inviting me to participate in this hearing and I would be pleased to answer any questions you might have.

Statement of Dr. Stuart H. Starr

It should be noted that the findings and recommendations in the studies cited in this testimony represent the work of individual researchers and do not necessarily represent the view of the National Defense University, the Center of Technology and National Security Policy, or the Department of Defense.

Mr. Chairman, distinguished Committee members, ladies and gentlemen. I am pleased to have the opportunity today to address this Sub-Committee on the important topic of actions to enhance the use of commercial Information Technology (IT) in Department of Defense (DoD) systems. To explore that issue, the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU), has pursued an aggressive IT study program over the past four years. We have conducted a structured set of nearly forty (40) coordinated activities that has leveraged the insights developed by the most creative members of government, industry, academia, and think tanks. I would like to submit for the record, a report that we have generated at CTNSP that summarizes the individual activities and captures the major findings and recommendations from those efforts (Reference 1).

Today, I would like to highlight key insights that we have derived from those efforts. As a foundation, I will set the stage by discussing the key attributes of commercial IT products. I will then identify six broad obstacles that impede DoD's ability to capture IT capabilities developed outside the traditional defense acquisition process. In order to overcome those obstacles, I will then identify a multi-step approach that leads to the adoption of a balanced package of initiatives. I will then conclude my remarks by identifying additional activities that are currently underway in CTNSP to redress residual issues.

A. Setting the Stage

The IT sector is one of the most dynamic elements in the world economy. It is characterized by extraordinary creativity, broad product diversity, and compressed time to market. Based on CTNSP's many IT-related studies, it is concluded that the successful injection of IT is critical if DoD is to accomplish the broad spectrum of missions that it must perform and maintain the technological lead that it enjoys against current and projected adversaries. However, it is becoming apparent that much IT technological innovation is occurring outside the DoD acquisition process. Thus, if DoD can not exploit commercial IT effectively, it will miss major opportunities to capitalize on those technological innovations. This is particularly troublesome because existing and potential adversaries (e.g., global terrorist organizations, transnational criminals) have full access to the IT technological innovations that are emerging from commercial industry.

From DoD's perspective, Commercial-off-the-Shelf (COTS) products represent an important subset of commercial IT. If DoD is able to exploit COTS products effectively, it has the potential to acquire systems, more rapidly, with fewer resources. However, if these benefits are to be realized by DoD, it is important to identify key IT products early in their life-cycle. Early identification provides the opportunity to add features that are vital to the DoD at reasonable cost while the product is still malleable. As a caveat, however, note that if a COTS product is modified during a DoD acquisition, it is generally not covered by warranties and may not be compatible with future versions of the commercial product.

B. Major Obstacles

Six broad classes of obstacles have been identified that impede DoD's ability to capture IT capabilities developed outside the traditional defense acquisition process. These obstacles revolve around the facts that DoD constitutes a market for commercial IT products that is **non-attractive, non-transparent, non-agile, non-dominant, and isolating**. Furthermore, DoD's ability to tap commercial IT is limited by the attitudes of the prime contractors and Lead System Integrators (LSIs) that acquire major defense systems. Each of these obstacles is identified and discussed below.

1. Non-Attractive. As part of CTNSP's IT activities, we sponsored a survey of commercial IT firms that infrequently do business with DoD (Reference 2). In that survey, the firms that currently do not business with DoD cited the following major reasons for their reluctance to enter the DoD market:

- "They don't know what they want"
- "The application/bid process takes too long"
- "DoD only deals with large companies"
- "Our products are not needed by DoD"
- "We do not want to work with DoD"
- "There are too many barriers to the bid process"

Similarly, DoD conducted a study to identify why commercial IT firms are reluctant to do business with DoD (Reference 3). That study concluded that non-traditional defense firms are reluctant to enter the defense market because of intellectual property rights (IPR) issues (e.g., small firms are extremely reluctant to cede IPR to the Government); the long development times associated with defense procurements; and the onerous cost accounting, auditing, and oversight requirements levied by the Government.

2. Non-Transparent. In the CTNSP-sponsored survey cited above (Reference 2), current DoD contractors explained why they perceive the current DoD policies, processes, and procedures to be opaque.

- They noted that the process is too difficult, too slow, and too confusing.
- They decried the limited information that is available to small business.
- They noted the lack of opportunity for firms that have not won prior contracts.
- They observed that it is desirable to ease the security clearance process.
- They stated that the current DoD acquisition process is an exclusionary one.
- They complained that they lacked clear information about Government contracting.

3. Non-Agile. The planning, programming, budgeting, execution (PPBE) system requires the participants to predict technology transitions 18 to 24 months in advance. However, the program manager community cannot always predict the pace of innovation two years in advance and funding may not be available for fast-moving projects that are ready for transition. Consequently, a desirable science and technology (S&T) project may stall for 18 to 24 months, waiting for funding. This gap is often referred to as the "valley of death".

4. Non-Dominant. In the 1960s, the DoD was the dominant player in the IT market place. However, that situation has changed dramatically over the last decade. As noted in the Manager's Guide to Technology Transfers in an Evolutionary Acquisition Environment (Reference 3), "DoD is unable to acquire IPR for commercially developed technology, as it has done for defense-funded technologies in the past, because DoD's financial involvement will be limited and its demand is not dominant compared with the worldwide commercial market."

5. Isolating Market. Rhetorically, the DoD R&D community employs the mantra: "adopt, adapt, and develop" (i.e., first try to adopt commercial technology; if that is inadequate, try to adapt commercial technology to meet military needs; if that fails, develop military-unique solutions). Although that mantra is quite reasonable, there is a tendency to focus on the reasons why adopt or adapt are inappropriate and to jump to the development of military-unique solutions. In reality, the commercial sector is beginning to develop significant IT capabilities for the commercial sector that are more readily extensible to the military sector.

6. Primes/LSIs. During the course of ancillary studies (Reference 4), the roles of primes and LSIs were assessed with respect to the adoption/adaptation of commercial IT. Three specific issues were identified that suggest that primes and LSIs may be a potential obstacle in this area. First, prime contractors may have a natural tendency to prefer internal technology because they can see the design and make it work. Second, prime contractors may have conflicting objectives about adopting technology from an outside provider. This can range from something as intangible as the "not invented here" syndrome to more tangible issues, such as displacing the prime contractor's revenue base. In addition, primes may also be concerned about complex issues, such as problems with the timeliness and compatibility of technologies built by outside organizations. However, it should be noted that many LSIs make extensive use of commercial IT in their programs.

C. Recommended Actions

To overcome these obstacles, CTNSP has identified a balanced mix of initiatives for DoD to pursue (Reference 5):

1. Enhance communications/organization. To enhance communications, "technology prospectors" should be created to conduct more focused searches and facilitate the injection of COTS products into DoD systems. Web portals should be created to coordinate the use of commercial IT and "acquisition guides" should be provided to smaller companies to help them navigate the DoD acquisition process. Consistent with those recommendations, a new organization has been created at JFCOM. That organization, known as the Office for Research & Technology Applications (ORTA), has taken preliminary steps to coordinate the use of commercial IT and support these activities. However, it is lacking in adequate resources and authorities to fully pursue those activities.

2. Increase resource flexibility. Provide Combatant Commands (COCOMs) the ability to generate procurements using a joint task force (JTF) for COCOMs (perhaps led by JFCOM and NORTHCOM), building on the limited acquisition authority model provided to JFCOM by USD(AT&L) (Reference 6). The precise organizational relationship for the JTF should be decided by DoD; however, one option might be to place it under the Joint Staff. The Defense Security Cooperation Agency (DSCA) model for procurement should be emulated vice the creation of a new major acquisition group. A bridging fund should be created to support the acquisition of key commercial IT products.

3. Reduce acquisition barriers. Meaningful measures could include changing DoD rules on IPR and increasing thresholds for applying a simplified acquisition process. In addition, other transaction authority (OTA) should be adopted as the approach for commercial IT R&D and procurement.

4. Promote cultural change. This is a difficult task that might begin with increasing DoD education and training for commercial IT development and procurement, providing incentives for program managers and LSIs to use COTS, and adapting GAO-recommended best practices to acquire commercial-component business systems. The Defense Acquisition University (DAU) and the Industrial College of the Armed Forces (ICAF) could play a major role in the area of community education.

5. Review testing. Evaluate expanding Underwriter Laboratory-style testbeds (for product evaluation) and expanding operational testbeds to evaluate the impact of the technology on mission effectiveness. This role could be played by a Systems Engineering and Integration (SE&I) organization that would deal with broad system-of-system issues. This organization might be resident at the Defense Information Systems Agency (DISA) with strong COCOM participation.

6. Adopt requirements for specific missions. Explore opportunities for commercial IT to support specific missions such as stabilization and reconstruction operations (SRO) and homeland security. These opportunities are discussed below.

D. On-Going Activities

There are several on-going activities at CTNSP that are addressing residual barriers to the effective use of commercial IT in DoD systems. These include the creative use of commercial IT to enhance SRO, the development of a theory of cyberpower, the challenges that the US faces in the evolution of the Internet, and role of the US government in the governance of R&D.

1. Employing Commercial IT to Enhance SRO. CTNSP is exploring opportunities to employ commercial IT to enhance SRO. To shed light on this major challenge, CTNSP has recently developed two key products. First, it has produced a policy paper entitled "I-Power: The Information Revolution and Stability Operations" (Reference 7). This paper includes a discussion of an information and communications technology (ICT) business model to guide the coordinated activities of the many participants in an SRO. Versions of this paper have been presented to several COCOMs, and it is serving to provide the framework for a serious dialogue on the issue. Second, working in partnership with the staff of the ASD(NII), "A Primer on ICT Support for Civil-Military Coordination in S&R and Disaster Relief Operations" has been completed (Reference 8). It characterizes the existing ICT architecture, formulates options to ameliorate ICT shortfalls, and captures community best practices. Both products are living documents that must be expanded and evolved to guide the changes in this critical area.

2. A Theory of Cyberpower. CTNSP is conducting a study of cyberpower to help understand the consequences of developments in cyber infrastructure, content, and institutions on the balance of power with potential adversaries of the US. In the absence of such a framework, the US potentially will pursue fragmented, ill-coordinated cyber initiatives in the technical, operational, legal, governance, and policy domains. The results of this study will serve to provide the intellectual underpinnings for coherent actions in this vital area. In particular, it will provide a framework in which to explore the appropriate balance between government and commercial actions in areas such as critical infrastructure protection.

3. Evolution of the Internet. CTNSP staff members have begun to focus on the challenges that the US faces in the evolution of the Internet. From technical and operational perspectives, these involve the actions that the U.S. must undertake to reduce the vulnerabilities of the Internet to adversary actions. From a governance perspective, new mechanisms are required to ensure that the Internet needs of other nations are addressed without compromising the national interests of the US.

4. Role of the US Government in the governance for R&D. Recently, staff members at CTNSP issued a report entitled, "The S&T Innovation Conundrum" (Reference 9). That report distinguished between two distinct phases in S&T innovation. These two phases can be captured by the descriptors "prospecting" (during which period no functional capability is generally produced) and "mining" (where rapid technical progress resulting in significant new functional capability is possible with the application of adequate financial and human capital). It is argued that the proper role for the government in R&D is to ensure the health of the "prospecting" phase of R&D. This role is crucial for long-term economic growth and military power, but it is not going to get done by the private sector. In order for the government to play this role successfully, it is vital that it be staffed with world class scientists and engineers.

E. Summary

It is widely recognized in the defense community that advances in IT are the key to transforming the military from an industrial age, platform-oriented force to an information age, net centric force. In support of that understanding, the IT program at

CTNSP has created an extraordinary intellectual reservoir that can help DoD navigate that transformation effectively and efficiently. The cumulative value of the CTNSP work has been to support four objectives: clarify the nature of the IT problem that DoD faces; identify the needs of the users of this technology; identify and recommend actions to enhance the injection of commercial IT into DoD systems; and explore innovative ways of employing IT to enhance the effectiveness of future US Government operations.

The IT program at CTNSP is notable for two key features. First, it has enlisted a multi-disciplinary set of the most knowledgeable and experienced members of the technology and national security policy communities. These complementary views have served to clarify the major technical issues and to explore the impact of those issues on national security. Second, it has resulted in the generation and dissemination of a broad set of peer-reviewed products that have shaped the discourse on this critical area in the defense community.

References

1. Report to the Congress, "Information Technology Program" Center for Technology and National Security Policy, National Defense University, January 2006.
2. "Survey of Information Technology Firms", Schaefer Center for Public Policy, October 31, 2003.
3. Defense Procurement and Acquisition Policy, OUSD(AT&L), "Manager's Guide to Technology Transfers in an Evolutionary Acquisition Environment", January 31, 2003.
4. Kenneth Jordan, "Lessons Learned on Injecting Commercial IT into DoD Systems", CTNSP, NDU, January 2006.
5. Frank Kramer, Stuart Starr, and Larry Wentz, "Actions to Enhance the Use of Commercial IT in DoD Systems", Fifth IEEE International Conference on COTS-Based Software Systems (ICCBSS 2006), 13 – 17 February 2006, Orlando, FL.
6. Mike Wynne, Acting USD(AT&L), "Assistance to Commander, U.S. Joint Forces Command for Development and Acquisition of Certain Equipment", June 4,

2004.

7. Franklin D. Kramer, Larry Wentz, and Stuart Starr, "I-Power: The Information Revolution and Stability Operations", Defense Horizons Number 55, CTNSP, NDU, February 2007.
8. Larry Wentz, "A Primer on ICT Support for Civil-Military Coordination in S&R and Disaster Relief Operations", Defense & Technology Paper 31, CTNSP, NDU, July 2006.
9. Timothy Coffey, Jill Dahlburg, and Elihu Zimet, "The S&T Innovation Conundrum", Defense Technology Paper 17, CTNSP, NDU, August 2005.

DOCUMENTS SUBMITTED FOR THE RECORD

MARCH 14, 2007

Defense Horizons
Number 55
A publication of the
Center for Technology and National Security Policy
National Defense University
FEBRUARY 2007

I-Power: The Information Revolution and Stability Operations

Franklin D. Kramer, Larry Wentz, and Stuart Starr

Overview

Information and information technology (I/IT) can significantly increase the likelihood of success in stability operations—if they are engaged as part of an overall strategy that coordinates the actions of outside intervenors and focuses on generating effective results for the host nation. Properly utilized, I/IT can help create a knowledgeable intervention, organize complex activities, and integrate stability operations with the host nation, making stability operations more effective.

Key to these results is a strategy that requires that 1) the U.S. Government gives high priority to such an approach and ensures that the effort is a joint civilian-military activity; 2) the military makes I/IT part of the planning and execution of the stability operation; 3) preplanning and the establishment of I/IT partnerships are undertaken with key regular participants in stability operations, such as the United Nations and the World Bank; 4) the focus of the intervention, including the use of I/IT, is on the host nation, supporting host-nation governmental, societal, and economic development; and 5) key information technology capabilities are harnessed to support the strategy. Implementing the strategy will include 1) development of an information business plan for the host nation so that I/IT is effectively used to support stabilization and reconstruction; 2) agreements among intervenors on data-sharing and collaboration, including data-sharing on a differentiated basis; and 3) use of commercial IT tools and data provided on an unclassified basis.

Over the past 30 years, the information revolution has had an important impact on the conduct of military operations. In the United States, it has produced what is often called "netcentric warfare" or "netcentric operations"[1]—the combination of shared communications, key data, analytic capabilities, and people schooled in using those capacities—that has enabled enhanced joint activities, integrated distributed capabilities, much greater speed, and more effective maneuver. The result has been that the United States and its allies have been able to conduct very effective combat operations under a range of conditions, including quick insertion (Panama), maneuver warfare (major combat operations in Iraq), an all-air campaign (Kosovo), and a Special Forces–led effort (Afghanistan).

At the same time that major combat operations have proceeded so successfully, the United States and its allies have undertaken a variety of stability operations in Somalia, Haiti, Bosnia, Kosovo, East Timor, several African countries, Afghanistan, and Iraq.[2] These stability operations generally have included both economic and governance reconstruction and have spanned the full security gamut from nonviolent peacekeeping to full-blown counterinsurgency. Not one of these operations has approached the success achieved in combat operations undertaken in the same period.

This paper analyzes whether a strategic use of information and information technology (I/IT) in stability operations could lead to more successful operations. Certainly, the information revolution has been a dynamic and positive factor in business, government, and social arenas in the Western world. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types. This paper concludes that utilizing the elements of the information revolution in a strategic approach to stability operations would have positive results and sets forth the strategic and operational parameters of such an effort.

Problems of Stability Operations

Utilizing the fruits of the information revolution for effective stability operations requires a prior understanding of what makes a stability operation effective. As noted above, stability operations have security, economic, and governance reconstruction elements. Yet while it is widely recognized that stability operations go far beyond purely military actions—encompassing security, humanitarian, economic, and governance/rule of law issues—no one has set forth an actual strategic or operational doctrine that promises success in stability operations. As a World Bank staff report put it, "The Bank, like other international partners, is still learning what works in fragile states contexts."[3]

The problems of stability operations are evident. To begin with, no two circumstances are the same. To say that Haiti is different than Somalia is different than Bosnia is different than Afghanistan is only to hint at the depth and breadth of the complexities. These include the causes of the crisis that occasioned the intervention, the host-nation culture or cultures, the language or languages, the nature of the economies *ante bellum*, the influence of neighbors, and a multitude of other factors. By definition, the state structure has collapsed or is severely impaired. Often there has been significant violence. Internal groups have been factionalized and frequently have each others' blood on their hands. Economies are in disarray. Social mechanisms have broken down. Information is lacking, and communications mechanisms are limited.

Prior to almost all interventions, the international community already will have been significantly present in the form of international organizations, nongovernmental organizations, businesses, bilateral governmental activities, and many more venues. Once there is a major international intervention, complexity increases greatly. Regardless of the initial number of international actors, the number and diversity of participants increase. More importantly, their relative importance increases for such functionality as exists or is created in the host country. Additionally, whereas before the intervention, development often had priority, now there are simultaneous challenges in the security, humanitarian, economic, and governance arenas—and, if social needs may be separated from the foregoing, in the social arena as well. Because of the expanded requirements, there are numerous players. Personnel and equipment stream in from civilian and military components of the governments of the United States and other nations, international organizations, such as the United Nations (UN) and its many agencies, the North Atlantic Treaty Organization (NATO), the Organization for Security and Cooperation in Europe, the African Union, the World Bank, and others. Nongovernmental organizations also are involved, many of them in the humanitarian arena, as well as numerous others that participate in myriad aspects of reconstruction and development. Many businesses also get involved, either as contractors to national and international organizations or as participants in private ventures.

A very important aspect of the complexity is that dealing with the host nation has become more difficult. Governmental functions are broken, and the government is seen by many as illegitimate and not representative of all the people; its reach is generally limited, and it is ineffective in mobilizing domestic human and other resources.

A further complicating factor is that circumstances on the ground change over time in significant part in response to the intervention. (The transformation from liberator to occupier is a well-known problem for intervening forces.) Interventions generally last for years, and a decade is not unusual. Stability operations encompass not only security but also reconstruction, and reconstruction takes time. In addition to actual changes, managing expectations of both the intervenors and the host nation becomes extremely important. For example, there is a so-called "golden hour" of 6–12 months during which actions must support expectations and the local population must experience improvements in quality of life.

It is in this context that the question arises whether the application of the tools and content of the information revolution can have a positive effect on the outcome of a stability operation.

Opportunities for I/IT Strategy

As difficult as the circumstances of a stability operation are, the very complexity provides significant opportunities for the use of an effective information strategy built around the use of information technology. It is worth underscoring at the outset what may be an obvious proposition: that information and information technology have to be used together to be effective. One will not suffice without the other.

At the most basic level, information technology can be used to distribute information to important players in an ongoing stability operation. Making information available can have four important consequences.

First, it can *help create a "knowledgeable" intervention*. Even before the intervention, and certainly as the intervention progresses, the intervenors will need information of many kinds about both planned and ongoing respondent activities and about the host nation. For the latter, population characteristics, cultural dynamics, economic structures, and historical governance issues all can be described and analyzed.

The intervenors will first plan and then undertake many activities, with multiple players in each field of endeavor. While it will not be possible for all intervening actors to have the unity of command that is sought by militaries, the use of I/IT may allow for organizing a more common approach—or at least to reduce inconsistent approaches.

An information strategy supported by information technology provides an opportunity to share information among the stability operation respondents themselves. This sharing of information will facilitate the generation of a common approach and can help in the effective use of scarce resources. As an example, the allocation of health care resources might be usefully rationalized once there is at least a working sense of what types of resources are available from the respondents. Also, intervenors working on the rule of law in different sections of the country will be more effective if they adopt closely aligned approaches than if they use significantly different approaches, even if each is valid in and of itself.

A second key element of the strategy will be using I/IT to *help organize complex activities*. Normally, a stability operation will be undertaken on a countrywide basis. For even the smallest countries, this means a significant geographic arena, with all the difficulties of maintaining connectivity. The intervention also will undoubtedly extend over a significant timeframe, and I/IT will be necessary to maintain an updated approach as conditions on the ground change.

Complexity also will be manifested in the requirement to deal simultaneously with security, humanitarian, economic, and governance issues. Many intervenors will be involved in only one or some of these actions, but actions in one field often have consequences for another. Moreover, knowledge of what is happening in each is important for the development of an overall strategy capable of achieving an effective host nation. Even in a single sector, information supported by effective information technology would allow for more effective in-country coordination; and distributed players would be better able to take focused effective actions. Furthermore, knowledge is an important element in building trust and commitment among different stability operations players, which can be a key element in enhancing effectiveness.

Franklin D. Kramer (kramerf@ndu.edu) is a Distinguished Research Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University. Larry Wentz (wentzl@ndu.edu) and Stuart Starr (starrs@ndu.edu) are Senior Research Fellows in CTNSP.

The third key use of distributed information will be to *integrate the stability operation respondents with the host nation*. It bears stating more than once that the objective of a stability operation is not a "good intervention" but rather an "effective host nation" as a result of the intervention. To accomplish this difficult task, given that the host nation is likely fragmented, disrupted, and not very effective, the intervenors need to stay connected to the host nation so that the results are adopted and adoptable by the populace on whose behalf the effort is being undertaken. An I/IT strategy needs to involve the host nation (likely in numerous manifestations) in the ongoing activities of the intervention.

The fourth use of I/IT is to *integrate the host nation and make it more effective*. Effectiveness can be enhanced by using I/IT to identify key requirements and target scarce resources. Information for a budget process is an important example. I/IT will also be able to facilitate informed senior decisionmaking well beyond budget and budget-type decisions. For example, how best to bring previous warring factions to work together will involve important social and economic issues whose resolution can be enhanced by good information.

Host-nation capacity can also be created by the use of I/IT. Government operations can be reestablished with the proper use of information technology. Both the information systems and the training to use them will be required, but information capacity can be generated far more quickly than other infrastructures—and can enable other effective actions.

Key Questions for the I/IT Strategy

An important question in analyzing an I/IT strategy for stability operations is how such a strategy relates to what else is happening in the intervention. As noted by the World Bank staff, no one has developed a truly knowledgeable approach to stability operations, which, in World Bank parlance, is one type of activity in fragile states. There are, however, some principles that have been adopted by the international community and the United States that are worth noting here.

First, the international community, through the Organisation for Economic Co-operation and Development (OECD) and otherwise, has emphasized the importance of the principles of harmonization and alignment. *Harmonization* refers to having the outside intervenors work in a generally coordinated fashion. As the OECD Development Co-operation Directorate has stated, "Harmonisation is taken to refer to common arrangements amongst the donor community, rationalized procedures and information sharing between donors . . . related to the goal of greater coherence between and among donors."[4] *Alignment* refers to having the outside intervenors align their activities with the interests of the host nation. Again, as the OECD Development Co-operation Directorate stated, "Alignment has been defined . . . as a set of practices according to which donor organizations use recipient country strategies, policies, and practices . . . as a guide for their assistance programs."[5] Both these principles are embodied in the so-called Rome Declaration on Harmonization of 2003 and subsequent actions and statements of the major multilateral and bilateral donor entities and countries, including the United States.

I/IT can have an important, positive impact on both harmonization and alignment. Coordination among intervenors is one of the key achievable results of an effective information strategy implemented by information technology. Likewise, an I/IT strategy is an important element to ensure that the host nation is effectively integrated into the decisionmaking and implementing actions of the outside intervenors.

A second question is the relationship between an I/IT strategy and strategies for security, humanitarian needs, economic development, and governance/rule of law. The U.S. Government, and particularly the Department of Defense (DOD), has often talked about using all elements of national power for success in stability operations, often citing diplomatic, informational, military, and economic (DIME) power as key aspects of the types of power brought to bear by outside intervenors.

This so-called DIME paradigm is a useful model, although it is not meant to be exhaustive. For example, host-nation civil society may be affected by outside, nongovernmental, civil organizations that nonetheless are important elements of an intervenor's national power. Social issues also must be considered, and, unless "diplomatic" is read to mean all contacts other than military or economic, there will be important nondiplomatic interactions on matters such as rule of law. What the DIME paradigm shows most importantly, however, is that information needs to be considered in an overall context, just as the principles of harmonization and alignment indicate.

There is a sterile debate as to whether information only supports other activities or is an activity in and of itself. Certainly, information supports other activities. Military, economic, and governance activities all operate on the basis of information. Conversely, certain aspects of information, such as the establishment of technical structures, can be undertaken apart from other activities. As an example, think of the building of towers to create the infrastructure for a cellular network. Overall, however, information, as every other action in a stability operation, is designed for one purpose: to serve the objective of making the host nation effective. That is the overall context in which to consider I/IT and to determine whether and how to undertake a particular effort.

The broad challenge for an I/IT strategy for stability operations is to help create effective results from the multitude of players and actions that will be found in a particular situation. No one should think that information is a panacea. If a faction within a country resists working with another faction even after all information is exchanged, then that is a political problem and probably will not be solved by further information. But given that information is not a universal solution to all problems, the question is whether the information revolution can help harmonize, align, and make more effective the outside military and civilian governmental intervenors, international and nongovernmental organizations, businesses, and, especially, host nation in all its manifestations.

Elements of an I/IT Strategy

Five key elements are required to generate an effective I/IT strategy for the United States to use in stability operations.

Element 1. The first requirement is for the U.S. Government to make the fundamental decision that such a strategy is a key mandatory element of all stability operations. That is no small statement, because the reality is that the United States has never—in any of its many stability operations—made such a decision. But the rationale for such a conclusion is clear: information and information technology are crucial elements to the success of stability operations, supporting effectiveness, harmonization, and alignment goals.

A coherent U.S. Government I/IT strategy is essential to produce the needed results. This means that the effort has to be truly interagency—and, most importantly, be accepted as a key element by both DOD and the State Department (including USAID, the U.S. Agency for International Development). While some individuals have acknowledged this point, no such government-wide I/IT strategy exists, although a potential framework for one has been created.

Released by the President in December 2005, NSPD-44, "Management of Interagency Efforts Concerning Reconstruction and Stabilization," articulates the basic framework for interagency cooperation. It assigns primary responsibility for stabilization and reconstruction operations to the Secretary of State (through the Office of the Coordinator for Stabilization and Reconstruction) and mandates close coordination with DOD to integrate stabilization and reconstruction contingency planning with military planning, when relevant and appropriate. The Director of Foreign Assistance, who reports directly to the Secretary of State, also serves as the Administrator of USAID, where several offices have been created or restructured to deal with stabilization and reconstruction challenges.

At DOD, the framework was supported in November 2005 by the release of Directive 3000.05, "Military Support for Stability, Security, Transition and Reconstruction Operations," which affirms that such activities represent a core DOD mission and are given a priority comparable to combat operations.

Within this framework, however, the focus on I/IT has been limited. USAID, recognizing the potential of I/IT in stability and reconstruction operations, has taken some steps to include I/IT as a sector and development tool. USAID strategy states that it seeks to leverage I/IT in conflict management and mitigation missions and in humanitarian assistance operations. USAID also seeks to promote global access to IT and to assist development through several ongoing projects such as the Leland Initiative for Africa, the Digital Freedom Initiative, and the Administrator's Last Mile Initiative.

Some important embassies have also taken I/IT steps. The U.S. Embassy in Afghanistan created the position of Senior Telecom Advisor to facilitate coordination among both military and civilian U.S. Government elements in country. In Iraq, DOD established the Iraq Reconstruction Management Office within the Embassy structure, and it, too, has a telecommunication advisor to unify I/IT efforts. These efforts are the beginning of a coherent U.S. Government approach to I/IT. A complete strategy would, however, require the Department of State/USAID to make I/IT a key element of strategy in stability operations. These I/IT initiatives are a good start, but are not an integrated strategy. They do, however, provide a basis on which to build.

Element 2. Although the problems of stability operations go far beyond military, the second element of an effective I/IT strategy recognizes that, doctrinally, the military requires an I/IT strategy as part of the planning and execution of any stability operation. Accordingly, in both joint and Service documents—plans and the rules and guidance for the development and execution of plans—an I/IT strategy is a required element.

As noted above, this approach is fully consistent with the military analysis of the DIME paradigm. The key point here is that military planners and operators need to include an I/IT strategy in their approaches. A subsidiary—but crucial—point is that an I/IT strategy is *not* a traditional function of the J–6 (the technical information officer on a military staff, the chief information officer in business terms). Rather, I/IT has to be a function of both J–3 and J–5: that is, built into plans and implementation and policy. The J–6 will be in a supporting/implementing role to help execute the strategy. There is no reason why the J–6 cannot help develop the I/IT strategy, but it cannot be developed apart from the policy, plans, and execution of the larger effort. This is not a technical problem; it is a strategic effectiveness problem to accomplish host-nation harmonization, alignment, and effectiveness.

The U.S. military has already taken some important steps in terms of using I/IT as part of a stability operation. Warfighting information technology is available if and when military operations are a required part of the stability operation. This paper does not deal with those issues and instead focuses on the issue of joint stability operations activity writ large—that is, joint within the U.S. Government and combined with other non-U.S. partners. On the latter, DOD has undertaken some very worthwhile efforts under the Combined Enterprise Regional Information Exchange System (CENTRIXS) program.[6]

CENTRIXS is a Web-based network, developed with both commercial off-the-shelf and government off-the-shelf tools. It is designed to provide information among coalition partners in activities in which the U.S. military is involved. For example, U.S. Central Command uses CENTRIXS to support coalition military coordination and information-sharing for the Multinational Force in Iraq and the International Security Assistance Force in Afghanistan. CENTRIXS operates on military classified networks, so it is not broadly available to all participants in a stability operation. It is, however, quite useful for information exchange among coalition militaries and is a good step in the direction of using information in stability operations.

Element 3. The third element of an I/IT strategy for the U.S. Government for stability operations is to pre-establish I/IT partnerships with key stability operations participants. It is important to underscore the word *key*. It is not possible, and would not be effective, to try to establish pre-existing partnerships with all of the many players who will be involved in a stability operation. But there are some very key players from the government perspective.

A few countries can be expected to participate in many and even most operations that the United States does. The United Kingdom is one; Australia is another. Certain key international organizations likewise will be there. The UN certainly would be involved—though dealing with the UN requires dealing with a variety of UN groups and agencies, since it does not act as a single entity. Thus, planning will be important with the Office for the Coordinator of Humanitarian Affairs, the UN Development Program, the UN Department of Peacekeeping Operations, and perhaps the UN Children's Fund. NATO is often a player, as well as the European Union. Major nongovernmental organizations will also regularly be engaged in stability operations. In fact, these organizations will generally be there in advance of the U.S. military. The fact that preplanning only includes some players is meant to allow for creation of a useful framework. An effective I/IT strategy will include many others, and there may be conferences, meetings, and workshops of a broader nature. But real planning will be enhanced by a more limited approach.

Element 4. The fourth element of an effective information strategy is to focus on the host nation. The importance of establishing host-nation effectiveness has already been emphasized. Informing host-nation decisionmaking, enhancing governmental capacities, and supporting societal and economic development are all crucial elements of an information strategy. Working with I/IT as discussed below can help generate important progress in security, humanitarian, economic, and governance/rule of law arenas. The recognition by the international community of the harmonization and alignment goals is important. However, when information technology is considered, all too often harmonization with respect to the intervenors becomes emphasized as compared to alignment and effectiveness of the host nation. This is backwards. An effective I/IT strategy is one that makes the host nation effective. Nothing else will do. Thus, a critical element of the strategy is an I/IT business plan for the host nation and an intervenor support strategy that aims to enable the host-nation business plan.

Element 5. The last element of an I/IT strategy will be to work with others to use the key technical capabilities to support the effectiveness, harmonization, and alignment goals. The specifics are discussed below, but a crucial point is that generating the technical part is far less about invention—the information revolution has given us and continues to give us broad capabilities—than it is about developing ways to use those brilliant inventions in an overall effective, collaborative fashion. The planning aspects of the strategy are crucial to effective use of the tools. Common choice can create highly effective capabilities. Divergent choices can undercut well-meaning strategies.

Operationalizing the I/IT Strategy

It is one thing to have a strategy; it is quite another to implement it effectively. The discussion below sets forth how to implement an operational I/IT strategy. A key point is to remember that both the end goal (creating an effective host nation) and the strategic context (the I/IT strategy itself) must be developed and implemented inside an overall approach of harmonization and alignment that supports enabling the host-nation security, humanitarian, economic, and governance activities.

To effectuate those tasks, the U.S. Government needs to adopt an information business model with multiple key elements. Those who have responsibility for the I/IT strategy, which ideally will be a joint effort led by the Department of State (including USAID) and DOD, will need to run the business model in a focused, long-term fashion; otherwise, achievement of the strategic aims will be jeopardized.

The business model breaks down into two broad elements: harmonization among outside intervenors, and effectiveness and alignment for, and with, the host nation.

Harmonization. On the harmonization side, a good place to start operational analysis is to recall the complexity of the problem and the number of intervenors. As discussed above, an important element of the strategy is to undertake preplanning with key partners. There are four important elements of preplanning to achieve harmonization.

First, joint civil-military information planning will be critical. In the first instance, this needs to be done between the Department of State and DOD, but most importantly it needs to be done between the U.S. Government and other major intervenors to harmonize their interventions. It is not an impossible task to keep others informed and aware, but it is difficult. Issues arise immediately as to what data can be provided and how information can be exchanged. With respect to the latter, development of agreed management and data standards can fundamentally enhance the provision of information. Pre-event planning and face-to-face meetings can enhance trust and provide important education about others' methods. While the myriad actual stability operations have provided some reasonable knowledge about different key actors, on-the-job learning is necessarily more difficult because of the requirement to do one's "day job." Accordingly, some common training, exercising, and/or education away from a stability operation can create potentially significant opportunities to enhance harmonization. None of this will occur unless an element of the government, preferably a joint Department of State-DOD element, focuses on the requirement for preplanning.

Second, improved collaboration depends on both better processes and use of available technical means. The process issue is perhaps the most crucial. As noted above, it is important to decide how, with whom, and how much data are shared. There is a general tendency, particularly at DOD, to come at the problem through a classified lens. That is, since DOD is used to treating data as classified, the question is often framed as how such data can be made available. Often, the answer is given in binary terms: information either can be made available or it cannot. This all too often becomes a least common denominator approach because the judgment is made that if the data are not available to some, it cannot be available to any.

A much better approach would be to recognize that, in stability operations, most relevant data are broadly available from other than classified sources—though often not broadly collected. Furthermore, and most importantly, data can be shared on a differentiated basis. For example, information provided to Japanese civilian officials can be differentiated from information provided to World Bank officials, which can be differentiated from information provided to Red Cross officials. Groups that have engaged in preplanning and have built up trust will find it easier to share information than groups that meet only in the circumstances of the stability operation. Differentiation is one key element to enhancing data-sharing—and working differentiation as an effective operational approach will depend on preplanning.

A second important step to better data-sharing will be better use of technical means. For example, the Internet has become a mechanism for unclassified collaboration and sharing of information among civilian and military elements responding to crisis operations. Furthermore, commercially available collaboration tools and other tools, such as video teleconferencing and Web-cams, are being used by them on the Internet. Technologies are improving quickly to enhance data-sharing. In the civilian arena, the growth of Web logs (blogs), file-sharing, Wikipedia, MySpace, and similar sites all attest to the possibilities of sharing, if the desire to use the mechanisms is there. Many organizations already run sites to make information available (for example, the UN-sponsored ReliefWeb). However, the collaborative aspects of these sites are limited.

U.S. Joint Forces Command (USJFCOM) has taken strides to enable the sharing of unclassified information with nontraditional partners. The command has conducted several exercises that explore this challenge, and Multinational Experiment 4 specifically addressed it. The command is also standing up a nonmilitary domain portal outside its firewall that takes an approach more akin to that of a relief organization—many of which are linked to it—than a military one. The portal (http://harmonieweb.org/) enables people and organizations who are participating in a relief effort to obtain and post information that may be valuable in providing the needed assistance.[7]

Additionally, the United States is encouraging the development of an open-source, collaborative arena, tentatively called "the hub," that would use blogging, file-sharing, and Wikipedia-type approaches to create an open space for collaborative sharing. It is not clear as of this writing what the outcome of that effort will be. However, even assuming its success, it seems probable that a combination of both a fully open site (the hub or some variant) and a more directed approach (for example, NATO–UN–World Bank collaborative sharing) might be useful. Remember the point about differentiation: to try to use only one tool or one kind of approach to allow for all types of collaboration is not necessarily the most successful approach. Transferring the CENTRIXS in some modified form for collaboration among key civil-military players while generating a broader open-source approach is likely to be a useful effort.

The third element required to achieve harmonization is the development of an implementation strategy. Whatever the precise mechanism for improved collaboration, it can be fairly confidently stated that improvements will not occur absent a strategy that designates elements within the government to make such improvements happen. At the moment, there are good but separate efforts. The Office of the Secretary of Defense is working on the hub effort. USJFCOM is seeking to support elements of the Department of State and, through experimentation, is developing new civil-military coalition processes for improved collaboration and information-sharing and assessing commercial information technology tools for enabling the processes. The recent DOD directive on stability operations requires development of a collaborative information-sharing mechanism.[8] But there is no overall directed effort—and this key element is crucial. Otherwise, the efforts will be personality-driven and ad hoc. Such approaches are way better than nothing but not likely enough to be effective.

An improved approach to collaboration includes broad agreement on the information needed to be collected and exchanged; standards for collection and exchange; technical mechanisms for each that work together; processes; and some education and training together. The final important element of collaboration is the ability to improve data usability. As noted above, it is probably useful to think about data in two broad types of collaborative forums: a more limited network among key partners, and a broader, more open network. In each, capacities for search, aggregation, storage, and retrieval are useful and potentially important. In each, the issues of quality control and information assurance will arise, as will the issue of dissemination.

Technical improvements in recent years have significantly increased the ability to aggregate different types of data, such as the ability to put written information on photographs and to integrate geographic material with other data. That said, there needs to be some data-management group that will determine for the collaborating activity just what kind of capacities will be created—or allowed. For example, it is possible to add to a photograph the names of the people in the picture, but in certain circumstances, adding names might be very hazardous for the individuals identified. An ongoing data-management effort to create rules and manage the activity will be necessary. There is, of course, a technical aspect to this, but some of the key issues will turn out to be policy issues, so the group will need to engage both technicians and policymakers.

Information power derives from a combination of people, content, and technical capabilities. In the technical arena, there is a whirlwind of ongoing activity and innovation. A very useful capability would be to have an "information toolbox" that maintains lists of:

- key information partners, including businesses with technical capabilities
- information and data-management tools
- other key tools, such as collaboration and translation.

For the effort that we are focusing on here, commercially developed tools are essential because government-generated tools will often not be available to important partners. There will be debates between open-source and proprietary tools, and those debates need to be resolved in actual context, based on what the effort is intended to establish. The case will probably be that the broader the activity, the more desirable the use of open-source—but even that statement needs to be evaluated in the particular circumstance.

The Center for Technology and National Security Policy at the National Defense University has generated a first order "tool kits and best practices" analysis in its recently published *ICT Primer*.[9] That discussion includes, inter alia, review of telecommunications capabilities such as satellite communications, creation of a civil-military information environment, data and information management, and best practices. Maintaining and updating such an activity is an important element of an overall strategy.

Effectiveness and Alignment. The fundamental task of an I/IT strategy is to enhance host-nation capacity. That is the critical result for which the stability operation is undertaken. To accomplish that result in an effective fashion, the strategy will need to accomplish two tasks, each familiar to the international community: first, assess the host nation and, second, establish a goal toward which to build. To put it more in the vernacular, a cure without a diagnosis will be improbable; directions without destination will be random. In short, an effective approach will require an information business plan for the host nation.

The assessment phase of an information business plan should begin before the intervention. It must include analyses of both information requirements and available information technology. Unlike humanitarian interventions, such as the relief effort for the December 26, 2004, tsunami, stability operations generally have long build-up periods, so there is time to prepare. An assessment would consider the pre-intervention state of information technology and information usage in the host nation. It is important to recognize that baselines will differ in different host nations. What can be accomplished in a country with an austere, pre-crisis baseline is likely considerably different from what can be accomplished in a more built-up, moderately established country. As an example, Bosnia is different from Afghanistan in terms of establishing an information business plan. Different baselines will generate different goals, and there will be no "one-size-fits-all" approach.

Some key elements of an information assessment will include evaluation of the host nation's telecommunications laws and regulations and communication infrastructures—land line telephone system, cell phone capacity, and Internet availability. It should also address usage patterns, language and literacy issues, technical training of locals, and financial resources.

Once an assessment has been undertaken, goals will need to be set for operationalizing the information business plan. Generally, it will be useful to time-phase the goals into an initial deployment phase, a middle phase (getting-things-going phase), and a long-term (exit-by-intervenors) phase. A critical point throughout is that the intervenors' information business plan goals need to be in support of the overall goals for the host nation, and the host nation as promptly as possible will need to help generate those goals.

The initial deployment phase will require the intervenors to consider what deployable capabilities will be useful to help establish a host-nation element or elements. There are both structural information capabilities, such as deployable cell phone capacities and the use of satellites, and functional capabilities, such as "health care in a box," that need to be considered.

The virtue of preplanning is that key intervenors can rationalize their capacities in the early, usually chaotic days of an intervention by considering which capabilities each might focus on. Equally important is to undertake such a discussion remembering that, first, numerous entities will already be in country with some capacities that can be utilized and that, second, host countries will likely have some capacity, and perhaps some significant capacity. Over the entirety of the intervention, the implementation of the information business plan likely will mean that the lead on different aspects of the plan will change. Broadly, one might expect a move from outside military intervenors to outside civilian intervenors to host nation, although the reality is likely to be more coordinated and complex. The transitions will occur over time, so there will be overlaps that need careful management. If it is understood from the beginning that there will be transitions in the way the plan is implemented, it will make for a more realistic and effective approach.

The middle phase of an information business plan for the host country will focus on five key elements. First is to *align the host country so that it is connected to the collaborative mechanisms used by the intervenors in some fashion*. While the key intervenors likely can use high-tech means, it may be that the host country will not be able to do so. An important task of an information business plan will be to allow for low-tech to high-tech connectivity. As an example, in Afghanistan, the literacy rate is so low that Internet use is necessarily limited and cell phone connectivity may be much more important. In fact, in Afghanistan, the cell phone is the lifeline communications capability. These points can be more broadly generalized: if the information business plan is to succeed, it must take account of the host nation's information culture and the related information technology culture.

A second element is to *help establish working government agencies*. Depending on the overall strategy, these could be central ministries or local/provincial offices. Information technology can be used to improve ministry effectiveness, especially to allow for an analytic approach through budgeting and transparency of expenditures. Those are crucial functions for the establishment of legitimate governance, and information technology can help each.

A third element for many stability operations will be to *increase connectivity between the central government and provincial/local governments*. Information technology can enhance this connectivity through, for example, the two-way flow of data and finances. Often, the cause of the crisis will have been differences between the central government and a region of the country, and working to bring warring elements together will be important. An information business plan can be an effective part of an overall effort.

A fourth element will often be to *provide certain important greater functionalities in government services to the populace*. While an information business plan may not be able to improve all functionalities significantly, health and education are two arenas of consequence in which such a plan can make an important difference. In the health arena, information technology can be used to build up local centers of health care, such as hospitals; support training of health care workers; and provide valuable functionalities, such as health surveillance systems. In the education arena, information technology can support curriculum establishment and the provision of instruction, as well as the training of teachers.

The fifth element is to *provide for the private-sector development of information capabilities*. Two of the most important issues are informed regulatory mechanisms and useful seed financing. An overly constrained regulatory environment will make it difficult for private enterprise to operate at a profit. A properly structured set of incentives can help create an environment in which profit-making companies can contribute importantly to economic reconstruction. Seed money may be very important, especially in the early days of a stability operation, particularly to get local involvement in the development of the information business plan.

The middle phase of the plan often may be the equivalent of the medical "golden hour" for establishing a framework for effective use of I/IT for the host nation. While the information flow may be limited, meeting expectations of the host government and population during this middle phase will be very important to longer-term success for the intervention and the host nation.

The middle phase will naturally flow over into the long-term phase for the host nation and the exit strategy for the intervenors. That part of the information business plan strategy should have at least three key elements. First, as noted above, the private sector should become a key element. Creating an environment in which there are commercial opportunities for information technology and information firms will help seed economic revitalization. Second, the host nation will need to consider what role it will play in the development of a national information technology infrastructure. Models range from full privatization to early phase ownership to ongoing involvement. Third, as part of their effort in country, intervenors will have established IT capabilities. Such facilities and datasets should not be automatically dismantled as the intervenors leave. Rather, they should be built as leave-behinds for local partners, both governmental and nongovernmental, whether commercial or nonprofit.

An I/IT strategy includes people, content, and technology. In a stability operation, the information needs—the content of what must be provided in addition to the connectivity—of the host nation require consideration. Broadly speaking, those information content needs will fall into the categories of security, humanitarian, economic, governance/rule of law, and social.

In analyzing how such information needs should be fulfilled, an I/IT strategy will recognize that the information element will support functional strategies for each of these arenas—all of which will have significant subparts. For example, the establishment of prosecutorial, court, and prison functions will have security and rule of law/governance aspects. Significant programs will be under way to help create each of these elements as part of a stability operation. Responding to the information needs of those programs has to be an affiliated strategic effort—or, to use the terms of the international community, needs to be aligned with the overall aims of the functional programs.

The specific needs may be provided with the use of information from one or more of the intervenors. In a variety of ways, information technology can be utilized to provide expert assistance. A simple example is maintaining an online list of experts. More sophisticated efforts can be established, such as a call-in center for the provision of various kinds of information. Research arrangements can be set up online, as can connectivity with key national and international organizations, both governmental and nongovernmental, that are willing and able to provide assistance.

As is true for the technology itself, information needs change over time. In fact, the ability to provide information may become more important as the host nation develops its own capacities. The capacity to access such information may be developed in two parallel fashions. First, in a traditional approach there could be an office to help facilitate access to expert management. More recently, a distributed approach, such as Wikis and blogs, may be able to make a great deal of expert information available without a specific data manager, if the right information tools are provided. Issues of trust and reliability will arise, but the community approach to providing information via the Internet has been very powerful in other arenas, and its use in stability operations should be encouraged.

The discussion of the management of information needs raises the important question of how to manage the I/IT strategy in the course of the stability operation. Adoption of a strategic approach and even operational activities will be greatly facilitated by the establishment of a forward field organization. Ideally, this would be a joint Department of State-DOD function with the job of carrying out the information strategy in country. In a stability operation, the organization likely would be collocated with the military command activity.

The role of the organization would include carrying out the U.S. Government aspects of the I/IT strategy. In addition, the organization would collaborate with the organizations with which preplanning took place, including key countries, the UN, and major nongovernmental organizations. As promptly as possible, the organization will want to begin to work with the host nation, though precisely what that means will depend on the circumstances of the operation. As a forward community of interest is being set up, the organization will want to create mechanisms that add to the effort entities that have not been part of the preplanning. As discussed above, a hub type approach may be very valuable, as may more structured relationships. In addition, the organization will want to work with the public affairs office to facilitate interaction with the media and, most importantly, information for the public at large.

Conclusion

I/IT can be important components for success in stability operations. Achieving successful results requires that a purposeful strategy be adopted to use these capabilities to the desired end of building up the host nation and to develop operational activities that effectively implement the strategy. A strategic approach causes coalition participants to undertake five key activities:

- conduct pre-event activities with partners
- implement improved collaboration
- ensure improved data usability
- develop an information toolbox
- create a forward field information office.

Also, creating an overall focus to generate an effective host-nation information business plan consists of four actionable items:

- assessing host-nation information capacity
- building a host-nation information goal
- creating immediate, medium, and long-term information capacities
- analyzing information needs and developing methods to fulfill those needs.

These activities and items can generate an environment in which the information revolution can help create success in stability operations.

Notes

[1] *Net-centric warfare*, as defined by the Department of Defense Functional Capabilities Board, refers to: warfighting that networks all elements of an appropriately trained joint force; integrates their collective awareness, knowledge, and experience in order to rapidly create new capabilities, make superior decisions, and achieve a high level of agility and effectiveness in dynamic and uncertain operational environments.

[2] Department of Defense (DOD) Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations*, Section 4.2, provides: "Stability operations . . . immediate goal . . . is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society." In this paper, the term *stability operations* is used per the DOD Directive to mean the full-spectrum of stabilization and reconstruction activities.

[3] World Bank, Operations Policy and Country Services, *Fragile States—Good Practices in Country Assistance Strategies*, December 19, 2005, vii, available at <www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2005/12/22/000090341_20051222094709/Rendered/PDF/34790.pdf>.

[4] Organisation for Economic Co-operation and Development, Development Co-operation Directorate, Senior Level Forum on Development Effectiveness in Fragile States, Harmonisation and Alignment in Fragile States, December 17, 2004, 14, available at <www.oecd.org/dataoecd/20/56/34084353.pdf>.

[5] Ibid.

[6] Jill L. Boardman and Donald W. Shuey, "Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide," available at <www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf>.

[7] Robert K. Ackerman, "Unclassified Information New Key to Network Centricity," *SIGNAL Magazine* (September 2006), available at <www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1185&zoneid=52>.

[8] DOD 3000.05, Sections 5.1.9, 5.7.1.

[9] Larry Wentz, *An ICT Primer: Information and Communication Technologies for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction*, Defense and Technology Paper 31 (Washington, DC: Center for Technology and National Security Policy, July 2006), available at <www.ndu.edu/ctnsp/Def_Tech/DTP31%20ICT%20Primer.pdf>.

Defense Horizons is published by the Center for Technology and National Security Policy. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk
Director

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 14, 2007

QUESTIONS SUBMITTED BY MR. SMITH

Mr. SMITH. 1) Mr. Lehman, please describe the unique role and capabilities of a Federally-Funded Research Development and Center (FFRDC). Why should the federal government maintain this construct as opposed to funding more research and development (R&D) internally or contracting it out to the for-profit private sector?

Mr. LEHMAN. DOD divides its FFRDCs into three categories, which differ in their roles and capabilities: (a) research and development laboratories, (b) study and analysis centers, and (c) systems engineering and integration centers. For example, the DOD C31 FFRDC, which MITRE operates, is a systems engineering and integration center; MITRE also operates FFRDCs for the Federal Aviation Administration and the Internal Revenue Service. My response focuses on the unique role and capabilities of systems engineering and integration FFRDCs, especially those supporting the DOD, but many of these points apply equally to other FFRDCs.

FFRDCs help our government sponsors to be ***smart buyers*** of systems and capabilities, understanding what technologies, systems, or commercial products will perform the most essential functions in the most reliable and cost-effective way. We are able to do this because:

- A set of limitations imposed by the Federal Acquisition Regulation, the DOD Management Plan for FFRDCs, and the Sponsoring Agreements with the DOD ensure that FFRDCs can be fully objective, with extremely strong protections against organizational conflict-of-interest. The major limitations are our not-for-profit status, a prohibition against manufacturing products, a prohibition against competing for any federal contract except for operation of an FFRDC, strict limitations on work for or teaming with any profit-seeking company, and a requirement that DOD or one of our other FFRDC sponsors approve in advance any work they undertake.
- FFRDCs are given a unique role with unusual access to government personnel, information, and future plans. Because FFRDCs do not compete with for-profit companies and have strong conflict-of-interest policies, for-profit companies are willing to share with FFRDCs proprietary information relevant to technologies being sought by the government.
- The status of FFRDCs as private corporations allow them to manage their technical workforce in accordance with industry practices, rather than the government model. In particular, they can make rapid decisions to hire, fire, promote, or transfer technical staff on the basis of the expertise needed for the tasks at hand. Additionally, FFRDCs can set compensation levels to reflect the market for each of the needed skill sets, including the possibility of rewarding careers for technical experts who have no interest in a management role.

FFRDCs enable the Defense Department and related elements of the Intelligence Community (IC) to ***integrate*** systems and technologies that were developed at different times, for different purposes. by different organizations. FFRDCs are able to do this because:

- Integration of disparate systems and capabilities is one of their major functions, whereas for most government program offices it is a secondary issue, and for industry it often looks like making a competitor's product more useful.
- They support many different DOD and IC organizations, and they are trusted to provide an objective, conflict-free account of the technical issues involved in making their systems work together effectively.
- The continuity of FFRDC efforts over many years means that they often have insights that government personnel lack into why a particular system was designed in a particular way.

FFRDCs are uniquely positioned to provide the government with a broad "architectural" view of government systems. In addition to strong government program offices, real progress towards integration requires effective problem definition, evaluation of alternative solutions and an analysis of execution feasibility. This requires an in-depth knowledge of the systems involved and how new systems can be integrated with legacy government systems. The long term relationship between FFRDCs and their government sponsors provides the basis for the development of an overarching plan (or architecture) for the integration of government systems and increases the likelihood of successful acquisitions.

FFRDCs as organizations combine depth of technical knowledge with the distinct mission ***to estimate risks*** accurately. One of the major difficulties faced by the DOD is that the most senior decision-makers, who want an objective assessment of the level of risk associated with each of the alternatives they must decide among, receive most of their information from organizations that have incentives either to be excessively optimistic about the cost, schedule, and technical performance of the capabilities they are selling or buying—or to overstate their resource requirements in order to achieve organizational growth. An FFRDC has no economic incentives to support the funding of one capability over another, and no bureaucratic incentives to see any organization increase its role or size. FFRDCs do, however, have incentives to be viewed as technically astute, objective, and trustworthy, and understand very well that the extent to which the DOD will want our support tomorrow will depend on their assessment of how good our technical support is today.

Mr. SMITH. 2) Mr. Lehman, what is the key to aligning R&D investments with the goals of an organization or the needs of the end user? How can this be assured? How can this situation be created in the DOD?

Mr. LEHMAN. The key is leadership from the top, measuring the success of organizational units on the basis of an overarching enterprise view, not simply their own organizational responsibilities. For instance, the person in charge of logistics can be doing an adequate job by fulfilling requirements that came from calculations when the prime mission equipment was in development. The warfighter focuses on the day-to-day duties using the prime mission equipment. It is the job of leadership to create dialogue among these organizations, so they are not simply trying to improve metrics that measure their individual success, but focus on metrics that measure the success of the entire enterprise.

Enterprise metrics have to be established and managers have to act to improve those metrics, which may entail real stress within an individual organization. For example, Hewlitt Packard uses the metric "percent of sales from new products." New products come from R&D, and R&D has to talk to Sales about what customers are demanding. Products have to be built efficiently, so Manufacturing is also part of the dialogue.

Results of the dialogue may be painful. An R&D lab may have to shed a whole group of employees in a skill area that was important ten years ago but is no longer relevant (an action not possible under the current civil service system). It may have to kill a favorite project. Logisticians may find when in continuous dialogue with warfighters using the equipment they support that they have been producing more of one kind of part and not enough of another, thus forcing labor dislocations in the private sector. These arc all hard decisions for managers, and it takes leadership from the top to act internally for the good of the enterprise.

This kind of leadership cannot be assured in business, and it cannot be assured in the DOD. Large organizations cannot expect behavior changes by simply declaring the expected result. Desired behaviors must be incentivized, rewarded, and held up as examples for others.

Congress could help. The growth of earmarking has made it increasingly difficult for DOD leadership to take a strategic view of R&D priorities. It would greatly change the atmosphere within DOD if Congress began to send signals that alignment of R&D with the most important needs of the end-user is more important than preserving R&D projects in Members' districts. It would also help if the rules for reprogramming funds during the year of execution provided incentives for DOD managers to hold costs below the budgeted amount.

Mr. SMITH. 3) Mr. Lehman, has there been an erosion in management expertise within the DOD? If so, what is the current state of this situation? Has it reached catastrophic proportions?

Mr. LEHMAN. I know many very good managers in the DOD. Congress has recognized the erosion in the acquisition force from retirements, lack of funding, and the inability to compete with industry salaries for talent. Congress has already taken action to correct this situation, but it will take time. Good acquisition managers require experience as well as training. The acquisition field has never been viewed as a path of advancement to the highest levels in DOD. Establishing acquisition as a career track with positive rewards would increase the incentive to remain and gain experience in that area.

Making civil service salaries more competitive with private industry, while initially costly, could provide substantial savings in the future by providing the DOD with an experienced cadre of acquisition managers and reduce the financial incentive for experienced government personnel to move to the private sector.

Mr. SMITH. 4) Mr. Lehman, you cite DOD's budgetary documentation and review process as having an adverse impact on innovation. Assuming we were to modify and perhaps streamline this process to create a more "positive development environment," how might we guard against the ills of improprieties and conflict-of-interest abuses?

Mr. LEHMAN. The DOD is a very large organization, and you cannot legislate a process that will make improprieties impossible. The rules are already in place. There will always be those who want, and will try, to cheat the system, regardless of the level of regulation. If someone infringes on the rules, prosecute them to the full extent of the law. The DOD audits, regulations and reporting requirements make it very difficult for small innovative companies to contract with the DOD; they do not have the overhead resources and financial structure to handle it. These companies end up subcontracting to the primes, and the government loses the opportunity for direct interaction with the innovation and innovative thinking of these companies.

Streamline the system. Yes, there will be abuses but many of these abusers will be caught and prosecuted, and that will deter others. Responding to every abuse with a new regulation makes the system cumbersome in ways that cost the taxpayers far more than a few bad people could steal.

Mr. SMITH. 5) Mr. Lehman, can you be more specific about how research schedules are not aligned with acquisition schedules? Please cite a few examples.

Mr. LEHMAN. Research projects have uncertainty of outcome and time and may fail entirely. But all research programs must have some failure or the program is probably not taking enough risk. They may not obtain the hypothesized results on the timeline the researcher expected, either for practical reasons like delays in equipment delivery, or scientific reasons like encountering unanticipated results.

This uncertainty means that usable results from a research project cannot be predicted to the accuracy required for an acquisition program to plan program expenditures. Acquisition programs have a contractor, a contract, a schedule, and a budget, all of which make it difficult to change course and accept a new result from a lab or industry.

On the other hand, when DOD labs start with 6.1, 6.2, or 6.3 research money, and solve a problem which begets an acquisition program built around the solution, the process works well.

Labs build their research program from requirements developed in a systematic process. Unfortunately, it usually lacks tight coordination with programs of record that might use their results too late in the acquisition process. What is needed is a fund at the program offices' disposal to harvest technologies when they mature to enable more effective transitions from labs to programs of record. See answer to question 8 below.

Mr. SMITH. 6) Mr. Lehman, is the for-profit private sector unwilling or unable to reform itself to provide the most-capable, most-innovative product?

Mr. LEHMAN. I do not think the for-profit sector is unable or unwilling to reform itself. The for-profit-sector responds to the incentives in the market. Change the incentives and the sector will change. The DOD has asked the for-profit sector for large acquisitions that small innovative companies cannot respond to. These acquisitions permit the contractor to develop a proprietary architecture that only that contractor can further develop and innovate. The contractors try to lock themselves in as the only contractor that can work on the system so they can make money on the long-term evolution and sustainment of the systems. They are doing nothing wrong; they are following the incentives in the market to make money for their stockholders.

The proprietary nature of these systems has been made worse over the years by such "reforms" as Total System Performance Responsibility, which required the contractor to have end-to-end accountability for how the system performed when fielded. In theory this is an excellent idea, but in practice the contractors refused to make government requested changes to open the architectures. The contractors quite rightly reasoned that they should not take accountability for total system performance for a system for which they did not have total design control. Large Scale Integration (LSI) contracts have further exacerbated this problem by the government's outsourcing of responsibility to control the architecture of the system being procured.

If the government controls the architecture and makes it open (i.e. all interfaces are well understood and available to all competitors), then the government can hire small (or large) innovative contractors to deliver capabilities into that architecture. The for-profit contractors will respond.

Mr. SMITH. 7) Mr. Lehman, precisely how can we encourage the DOD S&T, acquisition and user communities to manage the development process as a team?

Mr. LEHMAN. This question is similar to question 2, above, and I will elaborate on my answer there by emphasizing that the desired behavior can be achieved through incentives—recognition, promotion, cash awards, and publication of successes as examples for others to follow. Give the Service Secretaries a significant cash budget to award to those who develop cross-organizational or enterprise processes and metrics that lead to real results and cost savings. It does not need to be limited to aligning S&T, acquisition, and user communities. There are opportunities throughout the DOD, as there are in business, for better managing the enterprise.

Mr. SMITH. 8) Mr. Lehman, please explain your proposal to have a separate "innovation program element (PE) line" at the disposal of each program manager. How might this work in practice?

Mr. LEHMAN. If the R&D community investments are aligned with the acquisition program, we have solved half the problem—the R&D community is working towards solutions the acquisition community can use. However, their timing and success are unpredictable, as discussed in the answer to question 5 above. It is impossible for an acquisition program to budget against this uncertainty. I proposed a program element that would be available to acquisition programs upon request, when the technology matures, without having to wait two years to insert the request in the POM cycle. The programs requesting the funds would have to justify the return on investment to the warfighter. The adjudication of these requests could be done within each service's acquisition organization, with annual reporting to the committees of jurisdiction. To force proper prioritization, the fund should be large enough to accommodate some but not all requests. It should not be used to complete existing programs, but to insert innovations into existing programs.

Mr. SMITH. 1) The work of the Institute for Defense Analyses (IDA) in support of DOD's effort to secure domestic source production capacity for critical technologies is impressive. Might DOD have accomplished the success found in the "Trusted Foundry" effort without the assistance and guidance of an FFRDC? If not, why not? If so, why did this not occur?

Dr. COHEN. During the process leading up to DOD's decision to pursue the Trusted Foundry, there were conflicting perspectives offered by various people and organizations within the Defense Department, as well as by representatives of industry and Congress. IDA was asked to provide an independent, objective assessment of the issues. In doing so, IDA helped ensure that DOD's decision was based on the best available technical information, analyses and insights, provided by knowledgeable researchers and an organization with no financial or other interests in the outcome. This is a common role for FFRDCs like IDA. In recognition of this role, Congress often requests that FFRDCs conduct independent assessments of controversial issues, as evidenced by several studies in the FY08 Defense Authorization Act, including ones dealing with the size and mix of airlift forces, the roles and missions of the Missile Defense Agency, the civil reserve air fleet, and options for ballistic missile defenses in Europe. IDA helps the government make informed decisions. We defer to our sponsors to assess what might have happened in the absence of our support on any particular issue.

Mr. SMITH. 2) A 2005 Defense Science Board Study suggested the need for a "domestic Integrated Circuit competitiveness" policy as a national priority. Why is this important? In your view, what mechanisms would be necessary to adopt such a policy?

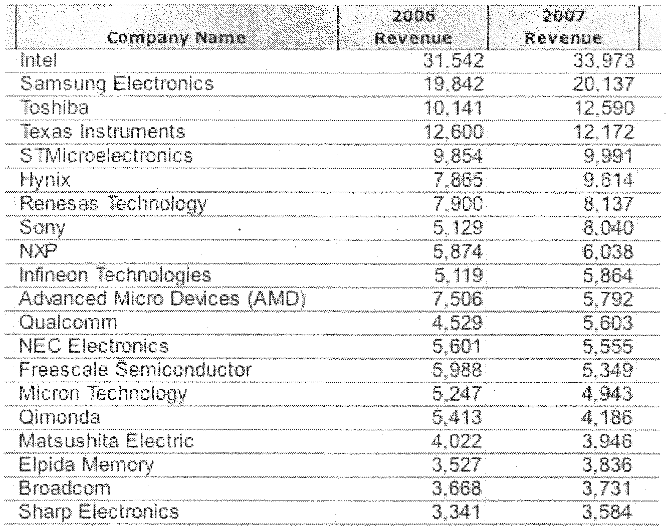
Dr. COHEN. A healthy domestic integrated circuit infrastructure would be desirable both for assured access and for lowering—though not eliminating—risks that adversaries might tamper with or exploit defense-related integrated circuits. The challenge has been finding practical solutions. It is important to note that there are a range of ways that DOD can manage these risks through its engineering and procurement practices and given support in the future through the use of new technologies such as those being explored by DARPA. In general, we agree with the DSB that many of the actions that would be required to address domestic integrated circuit competitiveness "*are beyond the scope and function of the department.*"

Global and commercial interests dominate today's integrated circuit market. As cited in the DSB report, defense purchases of integrated circuits are estimated to be 1–2% of the global market and even that small share is shrinking. Thus, the DOD demand for leading-edge integrated circuits is too small to influence business decisions in the largely volume-driven commercial market. DOD's demand is also too small to justify—based on business case analyses—developing and sustaining a captive capability, except perhaps for narrow elements in the supply chain.

One area where DOD has attempted to sustain domestic fabrication capabilities is in the supply of radiation-hardened electronics. Despite significant investments in two domestic suppliers, the lack of demand has hampered efforts to attain profitability. As a result, the radiation-hardened market sector lags significantly behind commercial capabilities in terms of transistor size. Moreover, even these radiation-hardened capabilities are not fully domestic, as the prime U.S. suppliers depend on a broad network of global secondary suppliers for equipment, materials and technology.

A major challenge has been addressing the cost of new advanced technologies, particularly as the feature sizes shrink down to 45nm[1] and below. A recent assessment[2] of semiconductor costs noted, *"at the 45-nm node, a new 300-mm fab costs about $3 billion, process technology R&D runs $2.4 billion and a "mask set" is up to $9 million."* This assessment further predicted that it would take annual sales of $13.3 billion to achieve a Return on Investment (ROI) at the 45nm technology level. This makes it challenging to get an acceptable ROI.

The projected IC ranking[3] of the top 20 suppliers of semiconductors in 2007 is shown in Figure 1. Given the high investment required for 45nm technologies, few companies are going to be able to justify investing in 45nm capabilities based on the current levels of revenue from sales of ICs. Further, only one or two domestic companies might be expected to have a business justification on their own to pursue these new technologies. The world leader Intel will likely have sales that support its pursing the next generation of technology on its own, but it is likely that much of the rest of the market will shift toward collaborative global alliances, sharing the costs and risks associated with the more advanced technologies.[4]



Company Name	2006 Revenue	2007 Revenue
Intel	31,542	33,973
Samsung Electronics	19,842	20,137
Toshiba	10,141	12,590
Texas Instruments	12,600	12,172
STMicroelectronics	9,854	9,991
Hynix	7,865	9,614
Renesas Technology	7,900	8,137
Sony	5,129	8,040
NXP	5,874	6,038
Infineon Technologies	5,119	5,864
Advanced Micro Devices (AMD)	7,506	5,792
Qualcomm	4,529	5,603
NEC Electronics	5,601	5,555
Freescale Semiconductor	5,988	5,349
Micron Technology	5,247	4,943
Qimonda	5,413	4,186
Matsushita Electric	4,022	3,946
Elpida Memory	3,527	3,836
Broadcom	3,668	3,731
Sharp Electronics	3,341	3,584

Figure 1. Preliminary Ranking of the Top 20 World-Wide Suppliers of Semiconductors in 2007 (Ranked By Revenue in $M) [3]

Given today's global commercial market place for integrated circuits and the high costs of creating and sustaining the next generations of technology, DOD is collaborating with selected domestic semiconductor suppliers as a way of continuing to mitigate security concerns.

[1] The most advanced IC technologies, now available from companies such as Intel contain transistors patterned with 45nm features. Intel processors at this features size became available in November 2007, (*http://download.intel.com/pressroom/kits/45nm/45nmSummaryFoils.pdf*)

[2] *Costs cast ICs into Darwinian struggle,* Mark LaPedus, EE Times, 03/30/2007.

[3] *Winners, losers in 2007 chip ranking,* Mark LaPedus, EE Times, 11/28/2007 (The market analysis in the article was provided by iSupply).

[4] IBM, Toshiba extend semiconductor R&D collaboration to 32nm, EDN Electronic News, Ann Steffora Mutschler, 12/18/2007 (IBM is reported to be partnering with Toshiba, AMD, Chartered Semiconductor Manufacturing Ltd., Freescale, Infineon and Samsung).

Mr. SMITH. 3) Please provide more detail about counterfeit components? How widespread and serious is this?

Dr. COHEN. Counterfeit semiconductor components are a serious concern not only for DOD, but also for the broader commercial electronics industry. A 2005 study by IDA[5] concluded, *"Counterfeit chips repeatedly have made their way through our supply chain and into deployed systems."* The broader commercial concerns also recently resulted in the Semiconductor Industry Association (SIA) creating the Anti-Counterfeiting Task Force (ACTF).[6] One conservative estimate of the dollar volume of counterfeit integrated circuits entering the DOD supply chain in 2005 was between $15 and $21 million.[7] The counterfeit efforts could involve a range of deceits, including remarking or relabeling parts, providing non-working or substandard parts, providing stolen parts, illegal manufacturing, establishing false provenance (from a different manufacturer, newer/older, or different part number or specifications like temperature range), overbuilding products, or actually reverse engineering and cloning.

DOD is paying more attention to the counterfeit problem and more significant numbers of counterfeits are being detected and reported. The GIDEP[8] acts as a clearinghouse for disseminating government wide reports of counterfeits. Figure 2 shows reporting rates throughout the government have increased dramatically.

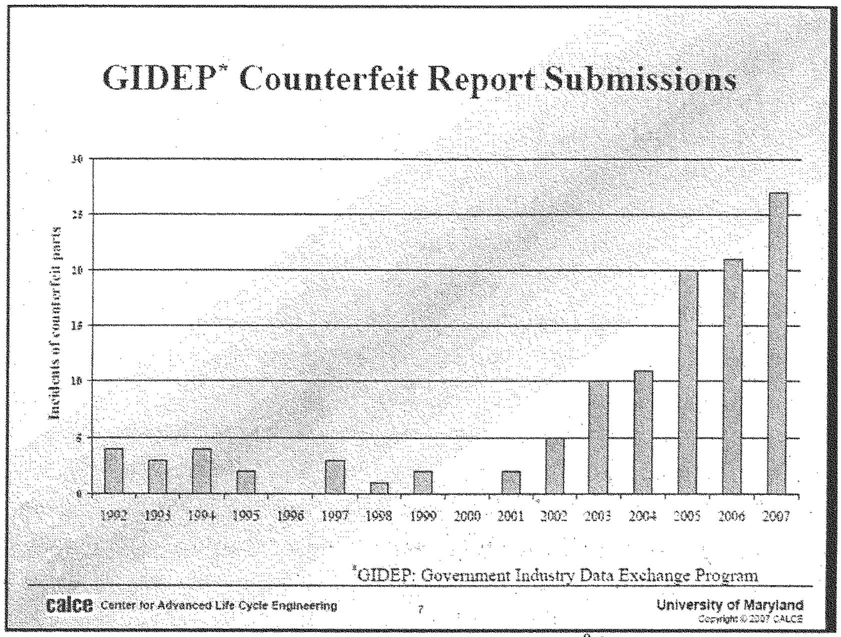


Figure 2. Counterfeit Reports[9]

[5] *USG Integrated Circuit Supply Chain Threat Opportunity Study,* FOUO, Donald J. Goldstein et al, IDA Document D-3222, January 2006, publication pending.

[6] SEMI and the SIA Launch SEMI Anti-Counterfeiting Standards Task Force at SEMICON West 2007, (*http://www.semiconwest.org/Showlnfo/LiveatWest/CTR 011164*)

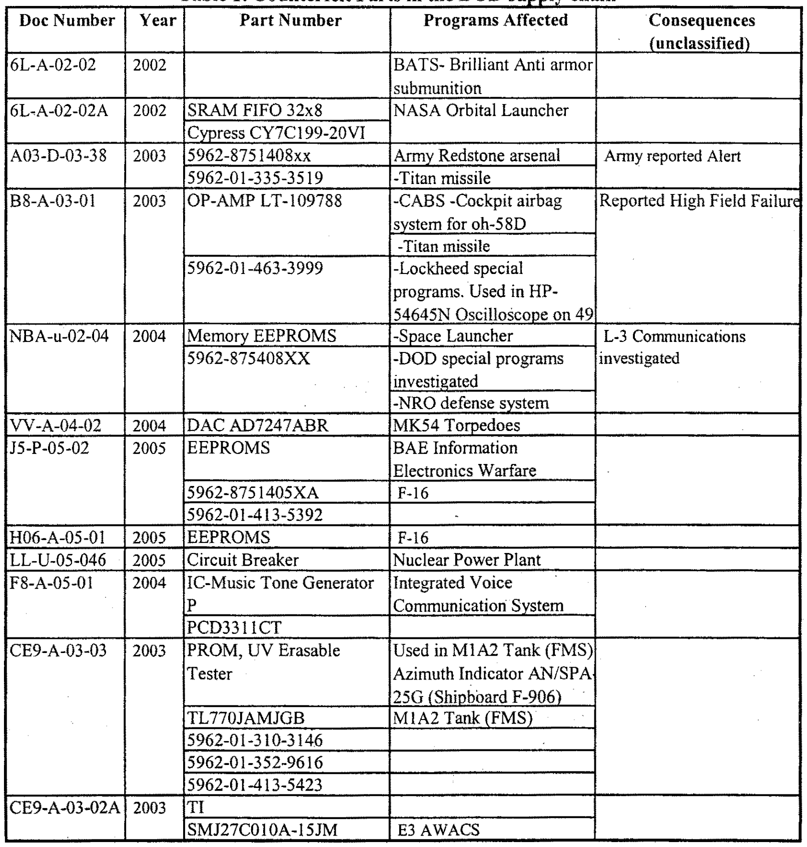
[7] Stradley, J.; Karraker, D., *"The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications."* IEEE Transactions on Components and Packaging Technologies, vol.29, no.3, pp. 703–705, Sept. 2006.

[8] GIDEP (Government-Industry Data Exchange Program) (*www.gidep.org*)

[9] *Counterfeit Electronic Parts,* Dr. Diganta Das, University of Maryland, DMSMS 2007 (*http://dmsms2007.com/media/proceedings/Gen__Sessions/Gen4__Thu/Gen4__Thu__1045__Das.pdf*)

Information from GIDEP was obtained as part of the 2005 IDA study[5] on the impact of counterfeiting on DOD systems, and reports on a number of counterfeit cases spanning the years 2002–2005 were provided. The results of IDA's inquiry are shown in Table 1. No doubt, a more current inquiry would result in a larger list. It is important to note that although programs are listed as being affected, this does not imply that there was any impact. In some cases, the parts were caught by existing processes and were not introduced into the operational environment.

Table 1. Counterfeit Parts in the DOD supply chain[10]



Doc Number	Year	Part Number	Programs Affected	Consequences (unclassified)
6L-A-02-02	2002		BATS- Brilliant Anti armor submunition	
6L-A-02-02A	2002	SRAM FIFO 32x8	NASA Orbital Launcher	
		Cypress CY7C199-20VI		
A03-D-03-38	2003	5962-8751408xx	Army Redstone arsenal	Army reported Alert
		5962-01-335-3519	-Titan missile	
B8-A-03-01	2003	OP-AMP LT-109788	-CABS -Cockpit airbag system for oh-58D	Reported High Field Failure
			-Titan missile	
		5962-01-463-3999	-Lockheed special programs. Used in HP-54645N Oscilloscope on 49	
NBA-u-02-04	2004	Memory EEPROMS	-Space Launcher	L-3 Communications investigated
		5962-875408XX	-DOD special programs investigated	
			-NRO defense system	
VV-A-04-02	2004	DAC AD7247ABR	MK54 Torpedoes	
J5-P-05-02	2005	EEPROMS	BAE Information Electronics Warfare	
		5962-8751405XA	F-16	
		5962-01-413-5392		
H06-A-05-01	2005	EEPROMS	F-16	
LL-U-05-046	2005	Circuit Breaker	Nuclear Power Plant	
F8-A-05-01	2004	IC-Music Tone Generator P	Integrated Voice Communication System	
		PCD3311CT		
CE9-A-03-03	2003	PROM, UV Erasable Tester	Used in M1A2 Tank (FMS) Azimuth Indicator AN/SPA-25G (Shipboard F-906)	
		TL770JAMJGB	M1A2 Tank (FMS)	
		5962-01-310-3146		
		5962-01-352-9616		
		5962-01-413-5423		
CE9-A-03-02A	2003	TI		
		SMJ27C010A-15JM	E3 AWACS	

There are other examples of counterfeit parts being sold to DOD.

In July 2005, two Florida men were sentenced to prison terms of 46 and 36 months respectively for selling to DOD counterfeit parts valued at between $4 to $12 million.[11] The counterfeit parts were sent to troops in Iraq and Afghanistan. The guilty parties admitted to sending thousands of parts to the Defense Supply Center Columbus (DSCC). A quality assurance specialist at DSCC said that while no loss of life can be attributed to this fraud, the actions delayed plans, sometimes for weeks and interfered with military operations. The two men started this operation when they learned how to bid on supply contracts over the Internet while

[10] Extracted by GIDEP records and communicated through personal communication by Stan Green, GIDEP to Vashisht Sharma (IDA), 20 July 2005.

[11] *Bogus military suppliers sentenced, St. Johns County men sold U.S. $4 million in phony parts sent to troops in Iraq, Afghanistan,* Florida Times-Union (Jacksonville), July 26, 2005, (*http://www.jacksonville.com/tu-online/stories/072605/met_19333168.shtml*).

attending community college in Jacksonville, FL. They would send substandard components to DSCC; when the parts were identified as defective, the men would simply change the name of their company and continue bidding. DSCC does not perform background checks on procurements of less than $100,000 and therefore was unable to track the men when they changed their companies' names.

In October 2007, a Florida man pleaded guilty to defrauding the DOD.[12] A federal judge ordered the man, who ran a St. Petersburg aerospace company, to spend two years in prison for selling used parts as new to the DOD. Prosecutors claimed that the government paid him $202,510 for 91 fraudulent contracts. The judge in the case ordered the defendant to repay that much in restitution.

Documents indicate that the defendant was president of Triton Aerospace between July 2004 and October 2005. Prosecutors said that the defendant fraudulently supplied parts for Navy and Air Force planes, including the B-52 bomber. The prosecutors claimed the defendant would shop around for surplus or overhauled parts, which he bought at a discount, and then in turn fraudulently sell them as new to the Department of Defense.

In summary, counterfeit components are entering the defense supply chain, and improved processes are detecting them more frequently. For instance, improvements by BAE to incoming inspections and testing have improved the detection of counterfeit parts.[13] BAE found that employing acquisition practices that monitor the provenance of parts and audit the origins of parts back to their original manufacturers reduces the opportunities for counterfeits to enter the supply chain. These types screening and authentication processes should mitigate much of the potential impact of the most damaging counterfeits.

Mr. SMITH. 4) It appears that policy recommendations include a relaxation of export-control measures in some areas and efforts to ensure more secure, domestic-production capabilities in other areas. When, where and how might we apply these two different approaches?

Dr. COHEN. The DSB report noted two approaches that could be employed to improve DOD's ability to meet needs for access to secure supplies of advanced integrated circuits: modifying export control and ensuring secure domestic production. The DSB report recommended that export controls be strengthened to assure "*that potential adversaries do not have access to leading edge design and wafer fabrication equipment, technology and cell libraries.*" This recommendation focused on strengthening export controls by, among other things, getting the U.S. government to persuade Wassenaar members to restrict exports of semiconductor material and equipment to China. As noted in the DSB report, U.S. attempts to do so have been rebuffed.

The DSB report also notes that "*Advanced semiconductor manufacturing and design equipment with roughly comparable performance characteristics is produced in a number of Wassenaar signatory countries. As a result, under the Wassenaar regime a Chinese buyer who cannot obtain desired equipment items from U.S. makers because the Department of Commerce has not granted an export license can often acquire comparable equipment from competing sellers based in Europe or Asia who are able to obtain licenses from their governments.*"

It is important to note that some important countries are not members of Wassenaar. In particular, Taiwan plays a dominant role in the global market for semiconductors and has a leading business position in the development of semiconductor manufacturing in China. This complicates the formulation of export control policies in this market area.

A recent IDA study[14] found that "*Semiconductor device firms and semiconductor materials and equipment firms did not report significant lost sales or competitive impacts from application of U.S. export controls.*" This is likely due to a climate of ongoing favorable licensing decisions by the Department of Commerce. The same report, however, noted, "*where U.S. export controls interfere with foreign partnering*

[12] Man gets two years in defense fraud case, October 13, 2007, St. Petersburg Times, *http://www.sptimes.com/2007/10/13/Hillsborough/Man__gets__two__years__in.shtml*

[13] BAE Systems: Counterfeit Electronic Components, Henry Livingston, DMSMS 2007, *http://dmsms2007.com/media/proceedings/Gen_Sessions/Gen2__Tue/Gen2__Tue__1035__Livingston.pdf*

[14] "*Export Controls and the U.S. Defense Industrial Base, Volume I: Summary Report and Volume 2: Appendices*", Richard Van Atta, Project Leader. Appendices, Van Atta et al, IDA Document D-3363, January 2007 (*http://handle.dtic.mil/100.2/ADA465592*)

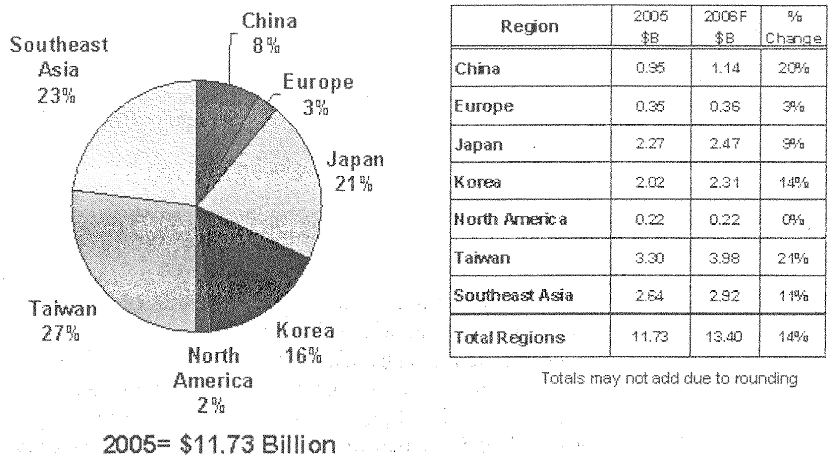
in high tech systems development, they encourage advanced technology and manufacturing investment to take place overseas." In summary, IDA found that "*As the locus of advanced IC consumption and production moves to Asia, including China as well as Taiwan and Korea, the underlying rationale for controlling microelectronics technologies appears to be negated.*"

It is not clear whether relaxation of export-control measures would have any impact on DOD's ability to obtain secure supplies of advanced ICs. In contrast, as I noted in my earlier testimony, the efforts to ensure more secure, domestic-production capabilities (primarily through the Trusted Foundry) have been quite successful in meeting DOD needs for secure advanced ICs.

Mr. SMITH. 5) You mention challenges in the field of packaging and circuit assembly. Please explain further.

Dr. COHEN. The assembly, test and packaging segments of the semiconductor supply chain were the first segments to move offshore. During the 1960s-1980s, much of the assembly, test and packaging moved to Taiwan, Hong-Kong and Malaysia, primarily for cost reasons.[15] Almost all packaging of integrated circuits—regardless of where the circuits are produced—is performed overseas, largely in Asia. Many companies vertically integrated these activities into their operations. Other companies outsource these elements of the supply chain, and some companies outsource the entire packaging, test and assembly portion.

In the packaging market, a good way to estimate the amount of packaging being performed in various parts of the world is to look at the sales of packaging materials. Plastic is the most frequently used material for packaging ICs and as shown in Figure 3, almost no large-scale plastic packaging takes place in North America. Even American firms will often package products overseas for cost reasons.



Region	2005 $B	2006F $B	% Change
China	0.95	1.14	20%
Europe	0.35	0.36	3%
Japan	2.27	2.47	9%
Korea	2.02	2.31	14%
North America	0.22	0.22	0%
Taiwan	3.30	3.98	21%
Southeast Asia	2.64	2.92	11%
Total Regions	11.73	13.40	14%

Totals may not add due to rounding

Figure 3. Regional Plastic Packaging Material Markets (Excludes Ceramic Packaging)[16]

The outsourced semiconductor assembly and test market is also mainly located in Asia as shown in Figure 4. There remain significant operations in the U.S. with Amkor, which has headquarters and significant operations located in the U.S. However, nine out of top ten outsourcing firms in this market segment are in Asia.

[15] "*U.S. Semiconductor and Software Industries Increasingly Produce in China and India*", GAO Report, GAO-06-423, September 2006.

[16] *Packaging Materials: Regional Markets,* Dan Tracy and Jan Vardaman, Semiconductor Equipment and Materials International (SEMI), (*http://wps2a.semi.org/wps/portal/_pagr/103/248?docName=P037398*)

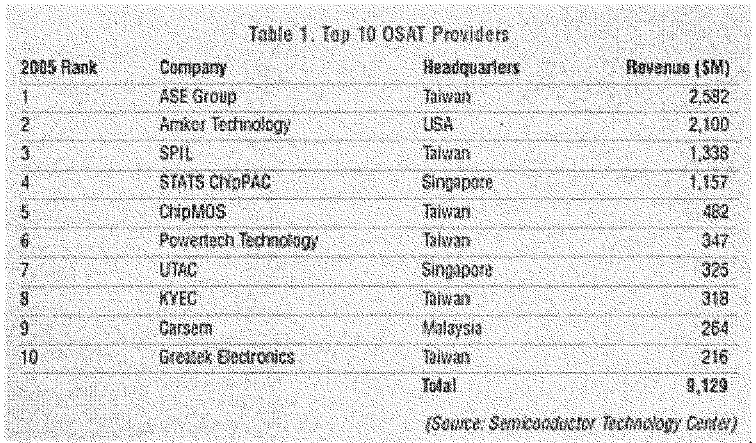


Table 1. Top 10 OSAT Providers

2005 Rank	Company	Headquarters	Revenue ($M)
1	ASE Group	Taiwan	2,582
2	Amkor Technology	USA	2,100
3	SPIL	Taiwan	1,338
4	STATS ChipPAC	Singapore	1,157
5	ChipMOS	Taiwan	482
6	Powertech Technology	Taiwan	347
7	UTAC	Singapore	325
8	KYEC	Taiwan	318
9	Carsem	Malaysia	264
10	Greatek Electronics	Taiwan	216
		Total	9,129

(Source: Semiconductor Technology Center)

Figure 4. Global Outsourced Assembly and Test (OSAT) Providers[17]

In 2000, there were concerns about the potential overseas migration of semiconductor wafer fabrication plants. The biggest concern was that it would be costly and time consuming to reestablish domestic semiconductor fabrication capabilities.

In the case of packaging, test and assembly, the situation is different, because the industry is much less capital and research intensive. There is little concern that U.S. would be denied access. Should the capability to perform these processes be disrupted, they could be reestablished domestically with less cost and delay. The security concerns are still important, and it is for this reason that DOD is interested in maintaining strong domestic packaging test, and assembly suppliers, rather than depending on a less expensive overseas-outsourced suppliers.

There continues to be sufficient domestic core competencies supporting defense needs as noted in the Linkages report by the NRC.[18] The report noted that "*Some very competent capability exists in a variety of places, such as (1) military facilities, including laboratories with limited production capabilities at the Warner Robins Air Logistics Center in Georgia and the Naval Surface Warfare Center, Crane Division, in Indiana; (2) small shops and boutique contractors; and (3) some defense prime contractors and their major subcontractors.*"

The Department, through the Trusted Foundry manufactures trusted integrated circuit dies[19] in the U.S. However, without secure on-shore assembly, test or packaging, these dies would have to be shipped overseas to a supplier for these steps, potentially compromising the security of these completed integrated circuits. It is in the Department's interest to address these issues by maintaining a core set of onshore trusted capabilities in assembly, test and packaging. This area has generally been manageable given the levels of specialized defense-related IC production that continue to reside in the U.S. DOD continues to actively monitor the situation.

Mr. SMITH. 6) You mention DARPA has pursuing a few promising research efforts in the field of circuitry security and access. How are the DARPA efforts encouraging and are there are promising efforts within DOD?

Dr. COHEN. A brief description of the DARPA Program follows.[20] Representatives of DARPA are the best sources of information on DARPA programs, and we would

[17] *Outsourced Semiconductor Assembly and Test '05: Boom Cycle Continued, but Profits Sagged,* ChipScale Review, Subash Khadpe, Contributing Editor, April 2006, (*http://www.chipscalereview.com/archives/0406/article.php?type=feature&article=f2*)

[18] *Linkages: Manufacturing Trends in Electronics Interconnection Technology, Committee on Manufacturing Trends in Printed Circuit Technology,* National Research Council (2005) (*http://books.nap.edu/catalog.php?record_id=11515*)

[19] A wafer is produced by a semiconductor foundry at diameters currently up to 300mm. The wafer, composed of many instances of individual chips, is then diced into individual chips, each of which is called a die. Each die is then "assembled" into a package and tested, thus producing a packaged integrated circuit.

[20] IDA has provided some focused technical assistance to DARPA in the formulation and solicitation processes for this program.

urge you to discuss this Program with them directly. DARPA is pursuing a TRUST in Integrated Circuits (Trust in IC) program to ".. *develop technologies that will ensure the trust of integrated circuits (IC) that are used in military systems but that are designed and fabricated under untrusted conditions.*"[21] This DARPA effort is by far the largest research effort throughout DOD focused on integrated circuit security concerns. The goal of the Trust in IC program is to provide assurance that an IC is free from maliciously inserted "*Trojan Horses*" that might disrupt operation, thereby affecting the confidentiality, integrity or availability of end systems. Attacks on ICs may take place anywhere in the supply chain, but the Trust in IC Program is addressing three of the most difficult elements of the supply chain. These elements are design, die fabrication and Field Programmable Gate Arrays.

This Program is being pursued because there is a belief that progress can be made in the elements. The ideal result of this Program would be a process that can be applied to achieve a quantified level of assurance that an IC obtained from an untrusted supplier is free from malicious tampering and will operate as intended. The program will have its initial four-month program review in March 2008.

Mr. SMITH. 1) You recommend greater resource flexibility and a greater role for the military combatant commands in the acquisition of IT systems yet you seem to stop short of granting these commands full acquisition authorities. Explain.

Dr. STARR and Mr. KRAMER. [In response to prior testimony before the HASC, six questions have been submitted for more detailed responses. Although specific testimony on the subject was provided by Dr. Starr, the principal investigators for the study on DOD use of commercial IT were Dr. Starr and Mr. Franklin D. Kramer. Thus the two of us have collaborated in preparing the responses to these questions. Note, however, that the answers represent the personal views of Dr. Starr and Mr. Kramer and they do not reflect the views of the National Defense University or any other U.S. Government entity.]

Our recommendation had two key parts. First, we recommended greater resource flexibility in the acquisition of IT systems. We made this recommendation because the current IT acquisition processes are too rigid and not easily adapted to dealing with commercial IT products. Second, we recommended that there be a greater role for the military combatant commanders (COCOMs) in the acquisition of IT systems. There are two key reasons why the military COCOMs should play a greater role in the acquisition of IT systems. First, it is vital to get them involved early in the process. By doing so, they can articulate their needs (to support their operations plans) and can state the unique constraints that are characteristic of their area of responsibility (e.g., interoperability with allies and coalition partners). Second, it is vital to get them involved continuously in evaluating candidate products and providing feedback.

However, we have several reasons for not granting COCOMs full acquisition authorities. In order to execute that responsibility, it requires key skills and experiences that are not generally present at COCOMs (e.g., systems engineering and systems-of-systems engineering). Furthermore, the COCOMs tend to focus more intently on near-term issues rather than on the longer-term planning horizon that is representative of major IT acquisitions. Thus, we believe that it would be extremely inefficient to have each COCOM take on this role.

However, we believe that Joint Forces Command (JFCOM) could assemble a "critical mass" in the needed intellectual capital and could focus on longer-term issues (consistent with its experimentation and testing activities). Thus, it should play the leading role for the COCOMs in the acquisition of commercial IT systems. [Note: We amplify on this expanded role for JFCOM in our response to Question 3]

Mr. SMITH. 2) Describe the acquisition model of the Defense Security Cooperation Agency (DSCA) and discuss how it might be used more broadly in the acquisition of IT systems.

Dr. STARR and Mr. KRAMER. The responsibilities of the DSCA are spelled out in DOD Directive 5105.65. That Directive notes the following:

"DSCA reports to the Under Secretary of Defense for Policy through the Assistant Secretary of Defense (International Security Affairs). DSCA serves as the DOD focal point and clearinghouse for the development and implementation of security assistance plans and programs, monitoring major weapon sales and technology transfer issues, budgetary and financial arrangements, legislative initiatives and activities, and policy and other security assistance matters through the analysis, coordination, decision, and implementation process. DSCA directs and supervises the organization, functions, training, administrative support, and staffing of DOD elements in

[21] "*DARPA TRUST IN INTEGRATED CIRCUITS PROGRAM*", DARPA News Release, December 2007, (*http://blogs.spectrum.ieee.org/tech__talk/trust__f__s.pdf*)

foreign countries responsible for managing security assistance programs and supports the development of cooperative programs with industrialized nations."

One of the Principal Investigators on the CTNSP Study Team had served as the Assistant Secretary of Defense (International Security Affairs) in the Clinton Administration. As such, he has had intimate involvement in the direction and guidance of DSCA. He observes that an analogous organization could be a highly efficient and effective mechanism to direct and guide the acquisition of commercial IT. The key point would be to create such an analogous mechanism to leverage the acquisition organizations of the Services to support the needed capability. Thus, one would have a lean focal point that would take full advantage of the acquisition organizations in the individual Services and Agencies.

Mr. SMITH. 3) What resources and authorities do you recommend for the Office for Research and Technology Applications (ORTA) at Joint Force Command (JFCOM)?

Dr. STARR and Mr. KRAMER. We would like to respond to this question by decomposing it into two parts. First we would like deal with the authorities issue. We will first characterize the authorities that ORTA currently has and contrast that with the authorities that we believe that they need to perform their job effectively and efficiently. Second, we will discuss the resources that ORTA needs to build upon those authorities.

In the area of Authorities, JFCOM currently has very little flexibility to support research or development of new technologies. They have found Cooperative Research and Development Agreements (CRDAs) to be useful, but limited. For example, both universities and small industries can not justify CRDAs because they need to receive some funding. In addition, JFCOM is currently under the OSD Small Business Innovation Research (SBIR) Program. However, we believe that they do not get benefits commensurate with their contribution.

To address these concerns, we believe that JFCOM should have greater technology transfer authority. These would include Other Transaction Authority and small Grant Authority with funds. In addition, we believe that JFCOM should have its own SBIR program.

In the area of resources, note that ORTA has recently expanded its staff size to five (i.e., three government personnel, one contractor, and one administrative person). We believe that its new size is probably sufficient for its current mission. These resources have enabled ORTA to effectively perform "needs" analyses. Note that JFCOM has Limited Acquisition Authority (LAA) for systems that are less than $50 million. However, we are aware that continuation of that authority is in question. In addition, JFCOM's LAA has never been accompanied by funding.

Looking to the future, we believe that the ORTA staff should be increased significantly to perform additional vital functions. For example, if ORTA is to be effective, it should undertake the following additional functions: perform "tech prospecting"; perform "gap" analyses and explore options to fill gaps; provide support to experimentation and testing; and work with rest of JFCOM to develop concepts of operations (in concert with J9/J7/JFHQ) and training packages (in concert with J7). In order to support those additional functions, it would be desirable to more than double the ORTA staff over a three year period.

Mr. SMITH. 4) A diffusion of system acquisitions has been cited as one cause of the DOD inefficiency in the realm of IT and a reason for more conformity and centralized decision-making with DOD.

Issues

- What is your view of this characterization?
- How does your recommendation to create a greater role and influence at the COCOMs support or undermine this proposal?

Dr. STARR and Mr. KRAMER. We believe that multiple processes are required. First, a "normal acquisition" process is needed that would address such vital issues as long term system-of-system engineering to ensure interoperability. In addition, there is a need for an "expedited acquisition" process that can take full advantage of commercial IT products to address immediate needs that emerge in key areas of operations.

We believe that the COCOMs have a major role to play in both processes. In the "normal acquisition process" they must be active participants in the requirements process (e.g., through the Integrated Priority List (IPL) process) and in the evolutionary acquisition of IT systems. In the latter case, they should get early versions of evolving systems and provide feedback to the acquisition agent (e.g., characterize how effectively the system is satisfying requirements; identify key functions that future systems should support).

In the "expedited acquisition process" the COCOMs should be active participants throughout the life cycle. This includes clarifying requirements, absorbing the new systems in their architectures, training personnel to use the new systems, and suggesting opportunities to improve evolving systems.

Mr. SMITH. 5) You recommend an increase in the threshold under which the simplified acquisition process might be applied to IT systems. At what level should this threshold be established?

Dr. STARR and Mr. KRAMER. In the Federal Acquisition Regulations (FAR) (dated 24 December 2007), the term "simplified acquisition threshold" is defined as follows:

"'Simplified acquisition threshold' means $100,000, except for acquisitions of supplies or services that, as determined by the head of the agency, are to be used to support a contingency operation or to facilitate defense against or recovery from nuclear, biological, chemical, or radiological attack (41 U.S.C. 428a), the term means—

(1) $250,000 for any contract to be awarded and performed, or purchase to be made, inside the United States; and

(2) $1 million for any contract to be awarded and performed, or purchase to be made, outside the United States."

Note that the threshold was initially established in Federal Acquisition Streamlining Act of 1994, P.L. 103-355, October 13, 1994.

We are aware that in Fiscal Year 2000, Congress authorized a test program to simplify the procedures for the acquisition of commercial supplies and services, allowing government buyers to eliminate certain procedural requirements when purchasing commercial items not exceeding $5 million. Subsequently, in April 2001, the GAO assessed that test program in a study entitled "Benefits of Simplified Acquisition Procedures Not Clearly Demonstrated". In that study, GAO cited a survey of procurement executives in federal agencies by the Office of Federal Procurement Policy that revealed "a positive impact on (1) time required to award a contract, (2) administrative costs, (3) prices, (4) small business participation, and (5) delivery of products and services." However, the GAO observed that "the survey did not collect empirical data that would have supported these views."

The GAO report made the following observations in the section "Matter for Congressional Consideration":

"Before providing permanent authority for using simplified procedures to acquire commercial items costing up to $5 million, Congress should consider extending the authority until 2005 and requiring the Administrator of the Office of Federal Procurement Policy to develop a method for demonstrating that the use of the simplified test program is producing the desired results. This demonstration project should be done in a fashion that would not deter government buyers from using the simplified procedures. This demonstration project should include an assessment of the extent to which (1) time required to award contracts was reduced, (2) administrative costs were reduced, (3) prices reflected the best value, (4) small business participation was promoted, and (5) delivery of products and services was improved."

In general, we agree with these observations by the GAO. We would conduct a test program that should run for five years. We would set the simplified acquisition threshold at $5 million for Fiscal Year 2009. However, we would index this number to the inflation rate to ensure that this threshold does not erode over the five year period. In addition, we would require an evaluation process of the five factors cited by the GAO.

Mr. SMITH. 6) You recommend a "bridge fund" for the acquisition of IT systems

- How large a bridge fund should this be?
- Would it be a Central Transfer Account?
- Who should manage and control it?

Dr. STARR and Mr. KRAMER. It is recommended that, to begin the process, the "bridge fund" should be on the order of $200 million to $300 million/annum for the following reasons. As we noted in our earlier testimony, the community is deeply concerned about the "Valley of Death" (i.e., the lack of resources to go from a good idea that has emerged from R&D into an acquired capability). To "bridge" this "Valley of Death", this "bridge fund" could used to provide timely resources to support key Test & Evaluation functions (particularly to ensure interoperability) and Sustainment (e.g., personnel training; upgrading systems as technology evolves). Ultimately, we believe that the precise size of the "bridge fund" should be based on successful performance (e.g., if it is used successfully and additional resources are needed, the fund should be increased to sustainable levels). Thus, it is vital to put in place a process that would continually assess the effectiveness of the "bridge fund" and help determine its appropriate size.

We believe that the "bridge fund" should be a Central Transfer Account. In addition, we believe that it would be appropriate for it to be managed and controlled by the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)).

○